

FortiConnect

Configuration Guide

Release 16.7

August 2016



Copyright© 2016 Fortinet, Inc. All rights reserved. Fortinet® and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

Support

For assistance, contact Fortinet Customer Service and Support 24 hours a day at +1 408-542-7780, or by using one of the [local contact numbers](#), or through the Support portal at <https://support.fortinet.com/>

Fortinet Customer Service and Support provide end users and channel partners with the following:

- Technical Support
- Software Updates
- Parts replacement service

Fortinet Product License Agreement / EULA and Warranty Terms



To ensure a secured WiFi network, Fortinet hardware (controllers and access points) are designed to run only the proprietary firmware developed by Fortinet. Only approved Fortinet access points are configurable with Fortinet controllers and vice versa. Third party access points and software cannot be configured on Fortinet hardware

Trademarks and Copyright Statement

Fortinet®, FortiGate®, and FortiGuard® are registered trademarks of Fortinet, Inc., and other Fortinet names may also be trademarks, registered or otherwise, of Fortinet. All other product or company names may be trademarks of their respective owners. Copyright © 2015 Fortinet, Inc., All Rights reserved. Contents and terms are subject to change by Fortinet without prior notice. No part of this publication may be reproduced in any form or by any means or used to make any derivative such as translation, transformation, or adaptation without permission from Fortinet, Inc., as stipulated by the United States Copyright Act of 1976.

Product License Agreement

The parties to this agreement are you, the end customer, and either (i) where you have purchased your Product within the Americas, Fortinet, Inc., or (ii) where you have purchased your Product outside of the Americas, Fortinet Singapore Private Limited (each referred to herein as "Fortinet"). CAREFULLY READ THE FOLLOWING LEGAL AGREEMENT (THE OR THIS "AGREEMENT" OR "EULA"). USE OR INSTALLATION OF FORTINET PRODUCT(S) AND ANY UPDATES THERETO, INCLUDING HARDWARE APPLIANCE PRODUCTS, SOFTWARE AND FIRMWARE INCLUDED THEREIN BY FORTINET, AND STAND-ALONE SOFTWARE PRODUCTS SOLD BY FORTINET (TOGETHER, THE "PRODUCTS") CONSTITUTES ACCEPTANCE BY YOU OF THE TERMS IN THIS AGREEMENT, AS AMENDED OR UPDATED FROM TIME TO TIME IN FORTINET'S DISCRETION BY FORTINET PUBLISHING AN AMENDED OR UPDATED VERSION. FORTINET SHALL NOT BE BOUND BY ANY ADDITIONAL AND/OR CONFLICTING PROVISIONS IN ANY ORDER, RELEASE, ACCEPTANCE OR OTHER WRITTEN CORRESPONDENCE OR OTHER WRITTEN OR VERBAL COMMUNICATION UNLESS EXPRESSLY AGREED TO IN A WRITING SIGNED BY THE GENERAL COUNSEL OF FORTINET. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS AGREEMENT, DO NOT START THE INSTALLATION PROCESS OR USE THE PRODUCTS. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, YOU SHOULD IMMEDIATELY, AND IN NO EVENT LATER THAN FIVE (5) CALENDAR DAYS AFTER YOUR RECEIPT OF THE PRODUCT IMMEDIATELY NOTIFY THE FORTINET LEGAL TEAM IN WRITING AT LEGAL@FORTINET.COM OF REQUESTED CHANGES TO THIS AGREEMENT.

1. License Grant.

This is a license, not a sales agreement, between you and Fortinet. The term "Software", as used throughout this Agreement, includes all Fortinet and third party firmware and software provided to you with, or incorporated into, Fortinet appliances and any stand-alone software provided to you by Fortinet, with the exception of any open source software contained in Fortinet's Products which is discussed in detail in section 15 below, and the term "Software" includes any accompanying documentation, any updates and enhancements of the software or firmware provided to you by Fortinet, at its option. Fortinet grants to you a non-transferable (except as provided in section 5 ("Transfer") and section 15 ("Open Source Software") below), non-exclusive, revocable (in the event of your failure to comply with these terms or in the event Fortinet is not properly paid for the applicable Product) license to use the Software solely for your internal business purposes (provided, if a substantial portion of your business is to provide managed service provider services to your end-customers, you may use the Software embedded in FortiGate and supporting hardware appliances to provide those services, subject to the other restrictions in this Agreement), in accordance with the terms set forth in this Agreement and subject to any further restrictions in Fortinet documentation, and solely on the Fortinet appliance, or, in the case of blades, CPUs or databases, on the single blade, CPU or database on which Fortinet installed the Software or, for stand-alone Software, solely on a single computer running a validly licensed copy of the operating system for which the Software was designed, or, in the case of blades, CPUs or databases, on a single blade, CPU or database. For clarity, notwithstanding anything to the contrary, all licenses of Software to be installed on blades, CPUs or databases are licensed on a per single blade, solely for one blade and not for multiple blades that may be installed in a chassis, per single CPU or per single database basis, as applicable. The Software is "in use" on any Fortinet appliances when it is loaded into temporary memory (i.e. RAM). You agree that, except for the limited, specific license rights granted in this section 1, you receive no license rights to the Software.

2. Limitation on Use.

You may not attempt to, and, if you are a corporation, you are responsible to prevent your employees and contractors from attempting to, (a) modify, translate, reverse engineer, decompile, disassemble, create derivative works based on, sublicense, or distribute the Software; (b) rent or lease any rights in the Software in any form to any third party or make the Software available or accessible to third parties in any other manner; (c) except as provided in section 5, transfer assign or sublicense right to any other person or entity, or (d) remove any proprietary notice, labels, or marks on the Software, Products, and containers.

3. Proprietary Rights.

All rights, title, interest, and all copyrights to the Software and any copy made thereof by you and to any Product remain with Fortinet. You acknowledge that no title to the intellectual property in the Software or other Products is transferred to you and you will not acquire any rights to the Software or other Products except for the specific license as expressly set forth in section 1 ("License Grant") above. You agree to keep confidential all Fortinet

confidential information and only to use such information for the purposes for which Fortinet disclosed it.

4. Term and Termination.

Except for evaluation and beta licenses or other licenses where the term of the license is limited per the evaluation/beta or other agreement or in the ordering documents, the term of the license is for the duration of Fortinet's copyright in the Software. Fortinet may terminate this Agreement, and the licenses and other rights herein, immediately without notice if you breach or fail to comply with any of the terms and conditions of this Agreement. You agree that, upon such termination, you will cease using the Software and any Product and either destroy all copies of the Fortinet documentation or return all materials to Fortinet. The provisions of this Agreement, other than the license granted in section 1 ("License Grant"), shall survive termination.

5. Transfer.

If you are a Fortinet contracted and authorized reseller or distributor of Products, you may transfer (not rent or lease unless specifically agreed to in writing by Fortinet) the Software to one end user on a permanent basis, provided that: (i) you ensure that your customer and the end user receives a copy of this Agreement, is bound by its terms and conditions, and, by selling the Product or Software, you hereby agree to enforce the terms in this Agreement against such end user, (ii) you at all times comply with all applicable United States export control laws and regulations, and (iii) you agree to refund any fees paid to you by an end user who purchased Product(s) from you but does not agree to the terms contained in this Agreement and therefore wishes to return the Product(s) as provided for in this Agreement. Further, if you are a non-authorized reseller of Products, you are not authorized to sell Product(s) or Software, but, regardless, by selling Product(s) or Software, you hereby agree you are bound by the restrictions and obligations herein and are bound to: (i) ensure that your customer and the end user receive a copy of this Agreement and are bound in full by all restrictions and obligations herein (ii) enforce the restrictions and obligations in this Agreement against such customer and/or end user, (iii) comply with all applicable United States export control laws and regulations and all other applicable laws, and (iv) refund any fees paid to you by a customer and/or end user who purchased Product(s) from you but does not agree to the restrictions and obligations contained in this Agreement and therefore wishes to return the Product(s) as provided for in this Agreement. Notwithstanding anything to the contrary, distributors, resellers and other Fortinet partners (a) are not agents of Fortinet and (b) are not authorized to bind Fortinet in any way.

6. Limited Warranty.

Fortinet provides this limited warranty for its product only to the single end-user person or entity that originally purchased the Product from Fortinet or its authorized reseller or distributor and paid for such Product. The warranty is only valid for Products which are properly registered on Fortinet's Support Website, <https://support.fortinet.com>, or such other website as provided by Fortinet, or for which the warranty otherwise

starts according to Fortinet's policies. The warranty periods discussed below will start according to Fortinet's policies posted at <http://www.fortinet.com/aboutus/legal.html> or such other website as provided by Fortinet. It is the Fortinet distributor's and reseller's responsibility to make clear to the end user the date the product was originally shipped from Fortinet, and it is the end user's responsibility to understand the original ship date from the party from which the end user purchased the product. All warranty claims must be submitted in writing to Fortinet before the expiration of the warranty term or such claims are waived in full. Fortinet provides no warranty for any beta, donation or evaluation Products, for any spare parts not purchased directly from Fortinet by the end-user, for any accessories, or for any stand-alone software. Fortinet warrants that the hardware portion of the Products, including spare parts unless noted otherwise ("Hardware") will be free from material defects in workmanship as compared to the functional specifications for the period set forth as follows and applicable to the Product type ("Hardware Warranty Period"): a three hundred sixty-five (365) day limited warranty for the Hardware excluding spare parts, power supplies, and accessories (provided, solely with respect to FortiAP and Meru AP indoor Wi-Fi access point Hardware appliance products and FortiSwitch Hardware appliance products other than the FortiSwitch-5000 series (for both excluding spare parts, power supplies, and accessories), the warranty herein shall last from the start of the warranty period as discussed above until five (5) years following the product announced end-of-life date), and, for spare parts, power supplies, and accessories, solely a ninety (90) days limited warranty. Fortinet's sole obligation shall be to repair or offer replacement Hardware for the defective Hardware at no charge to the original owner. This obligation is exclusive of transport fees, labor, de-installation, installation, reconfiguration, or return shipment and handling fees and costs, and Fortinet shall have no obligation related thereto. Such repair or replacement will be rendered by Fortinet at an authorized Fortinet service facility as determined by Fortinet. The replacement Hardware need not be new or of an identical make, model, or part; Fortinet may, in its discretion, replace the defective Hardware (or any part thereof) with any reconditioned Product that Fortinet reasonably determines is substantially equivalent (or superior) in all material respects to the defective Hardware. The Hardware Warranty Period for the repaired or replacement Hardware shall be for the greater of the remaining Hardware Warranty Period or ninety days from the delivery of the repaired or replacement Hardware. If Fortinet determines in its reasonable discretion that a material defect is incapable of correction or that it is not practical to repair or replace defective Hardware, the price paid by the original purchaser for the defective Hardware will be refunded by Fortinet upon return to Fortinet of the defective Hardware. All Hardware (or part thereof) that is replaced by Fortinet, or for which the purchase price is refunded, shall become the property of Fortinet upon replacement or refund. Fortinet warrants that the software as initially shipped with the Hardware Products will substantially conform to Fortinet's then current functional specifications for the Software, as set forth in the applicable documentation for a period of ninety (90) days ("Software Warranty Period"), if the Software is properly installed on approved Hardware and operated as contemplated in its documentation. Fortinet's sole obligation shall be to repair or offer replacement Software for the non-conforming Software with software that substantially conforms to Fortinet's functional specifications. This obligation is exclusive of transport fees, labor, de-installation, installation, reconfiguration, or return shipment and handling fees and costs, and Fortinet shall have no obligation related thereto. Except as otherwise agreed by

Fortinet in writing, the warranty replacement Software is provided only to the original licensee, and is subject to the terms and conditions of the license granted by Fortinet for the Software. The Software Warranty Period shall extend for an additional ninety (90) days after any warranty replacement software is delivered. If Fortinet determines in its reasonable discretion that a material non-conformance is incapable of correction or that it is not practical to repair or replace the non-conforming Software, the price paid by the original licensee for the non-conforming Software will be refunded by Fortinet; provided that the non-conforming Software (and all copies thereof) is first returned to Fortinet. The license granted respecting any Software for which a refund is given automatically terminates immediately upon refund. For purpose of the above hardware and software warranties, the term "functional specifications" means solely those specifications authorized and published by Fortinet that expressly state in such specifications that they are the functional specifications referred to in this section 6 of this Agreement, and, in the event no such specifications are provided to you with the Software or Hardware, there shall be no warranty on such Software.

7. Disclaimer of Other Warranties and Restrictions.

EXCEPT FOR THE LIMITED WARRANTY SPECIFIED IN SECTION 6 ABOVE, THE PRODUCT AND SOFTWARE ARE PROVIDED "AS-IS" WITHOUT ANY WARRANTY OF ANY KIND INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTY, IMPLIED OR EXPRESS WARRANTY OF MERCHANTABILITY, OR WARRANTY FOR FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT. IF ANY IMPLIED WARRANTY CANNOT BE DISCLAIMED IN ANY TERRITORY WHERE A PRODUCT IS SOLD, THE DURATION OF SUCH IMPLIED WARRANTY SHALL BE LIMITED TO NINETY (90) DAYS FROM THE DATE OF ORIGINAL SHIPMENT FROM FORTINET. EXCEPT AS EXPRESSLY COVERED UNDER THE LIMITED WARRANTY PROVIDED HEREIN, THE ENTIRE RISK AS TO THE QUALITY, SELECTION AND PERFORMANCE OF THE PRODUCT IS WITH THE PURCHASER OF THE PRODUCT. NOTWITHSTANDING ANYTHING TO THE CONTRARY, THE HARDWARE WARRANTY PERIOD DISCUSSED ABOVE DOES NOT APPLY TO CERTAIN FORTINET PRODUCTS, INCLUDING FORTITOKEN WHICH HAS A 365 DAY WARRANTY FROM THE DATE OF SHIPMENT FROM FORTINET'S FACILITIES, AND THE SOFTWARE WARRANTY DOES NOT APPLY TO CERTAIN FORTINET PRODUCTS, INCLUDING FORTIGATE-ONE AND VDOM SOFTWARE. YOU HEREBY ACKNOWLEDGE AND AGREE THAT NO VENDOR CAN ASSURE COMPLETE SECURITY AND NOTHING HEREIN OR ELSEWHERE SHALL BE DEEMED TO IMPLY A SECURITY GUARANTEE OR ASSURANCE. The warranty in Section 6 above does not apply if the Software, Product or any other equipment upon which the Software is authorized to be used (a) has been altered, except by Fortinet or its authorized representative, (b) has not been installed, operated, repaired, updated to the latest version, or maintained in accordance with instructions supplied by Fortinet, (c) has been subjected to abnormal physical or electrical stress, misuse, negligence, or accident; (d) is licensed for beta, evaluation, donation, testing or demonstration purposes or for which Fortinet does not charge a purchase price or license fee. In the case of beta, testing, evaluation, donation or free Software or Product, the end user acknowledges and agrees that such Software or Product may contain bugs or

errors and could cause system failures, data loss and other issues, and the end user agrees that such Software or Product is provided “as-is” without any warranty whatsoever, and Fortinet disclaims any warranty or liability whatsoever. An end user’s use of evaluation or beta Software or Product is limited to thirty (30) days from original shipment unless otherwise agreed in writing by Fortinet.

8. Governing Law.

Any disputes arising out of this Agreement or Fortinet’s limited warranty shall be governed by the laws of the state of California, without regard to the conflict of laws principles. In the event of any disputes arising out of this Agreement or Fortinet’s limited warranty, the parties submit to the jurisdiction of the federal and state courts located in Santa Clara County, California, as applicable.

9. Limitation of Liability.

TO THE MAXIMUM EXTENT PERMITTED BY LAW AND NOTWITHSTANDING ANYTHING TO THE CONTRARY, FORTINET IS NOT LIABLE UNDER ANY CONTRACT, NEGLIGENCE, TORT, STRICT LIABILITY, INFRINGEMENT OR OTHER LEGAL OR EQUITABLE THEORY FOR ANY LOSS OF USE OF THE PRODUCT OR SERVICE OR ANY DAMAGES OF ANY KIND WHATSOEVER, WHETHER DIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL (INCLUDING, BUT NOT LIMITED TO, DAMAGES FOR LOSS OF GOODWILL, LOSS OF PROFIT, LOSS OF OPPORTUNITY, LOSS OR DAMAGE RELATED TO USE OF THE PRODUCT OR SERVICE IN CONNECTION WITH HIGH RISK ACTIVITIES, DE-INSTALLATION AND INSTALLATION FEES AND COSTS, DAMAGE TO PERSONAL OR REAL PROPERTY, WORK STOPPAGE, COMPUTER FAILURE OR MALFUNCTION, COMPUTER SECURITY BREACH, COMPUTER VIRUS INFECTION, LOSS OF INFORMATION OR DATA CONTAINED IN, STORED ON, OR INTEGRATED WITH ANY PRODUCT INCLUDING ANY PRODUCT RETURNED TO FORTINET FOR WARRANTY SERVICE) RESULTING FROM THE USE OF THE PRODUCT, RELATING TO WARRANTY SERVICE, OR ARISING OUT OF ANY BREACH OF THE LIMITED WARRANTY IN SECTION 6 ABOVE, EVEN IF FORTINET HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE SOLE REMEDY FOR A BREACH OF THE LIMITED WARRANTY IS REPAIR, REPLACEMENT OR REFUND OF THE DEFECTIVE OR NONCONFORMING PRODUCT AS SPECIFICALLY STATED IN SECTION 6 ABOVE.

10. Import / Export Requirements; FCPA Compliance.

You are advised that the Products may be subject to the United States Export Administration Regulations and other import and export laws; diversion contrary to United States law and regulation is prohibited. You agree to comply with all applicable international and national laws that apply to the Products as well as end user, end-use, and destination restrictions issued by U.S. and other governments. For additional information on U.S. export controls see www.bis.doc.gov. Fortinet assumes no responsibility or liability for your failure to obtain any

necessary import and export approvals, and Fortinet reserves the right to terminate or suspend shipments, services and support in the event Fortinet has a reasonable basis to suspect any import or export violation. You represent that neither the United States Bureau of Industry and Security nor any other governmental agency has issued sanctions against you or otherwise suspended, revoked or denied your export privileges. You agree not to use or transfer the Products for any use relating to nuclear, chemical or biological weapons, or missile technology, unless authorized by the United States Government by regulation or specific written license. Additionally, you agree not to directly or indirectly export, import or transmit the Products contrary to the laws or regulations of any other governmental entity that has jurisdiction over such export, import, transmission or use. Furthermore, you represent that you understand, and you hereby agree to comply with, all requirements of the U.S. Foreign Corrupt Practices Act and all other applicable laws. For beta, testing, evaluation, donation or free Products and/or related services, you hereby agree, represent and warrant to Fortinet that (a) receipt of the Products and/or services comply with all policies and you have obtained all necessary approvals for such Products and/or services, (b) the Products and/or services are not provided in exchange for Fortinet maintaining current business or for new business opportunities, and (c) the Products and/or services are not being received for the benefit of, and are not being transferred to, any government entity, representative or affiliate.

11. U.S. Government End Users.

The Software and accompanying documentation are deemed to be "commercial computer software" and "commercial computer software documentation," respectively, pursuant to DFAR Section 227.7202 and FAR Section 12.212, as applicable. Any use, modification, reproduction, release, performance, display or disclosure of the Software and accompanying documentation by the United States Government shall be governed solely by the terms of this Agreement and shall be prohibited except to the extent expressly permitted by the terms of this Agreement and its successors.

12. Tax Liability.

You agree to be responsible for payment of any sales or use taxes imposed at any time on this transaction.

13. General Provisions.

Except as specifically permitted and required in section 5 ("Transfer") above, you agree not to assign this Agreement or transfer any of the rights or obligations under this Agreement without the prior written consent of Fortinet. This Agreement shall be binding upon, and inure to the benefit of, the successors and permitted assigns of the parties. The United Nations Convention on Contracts for the International Sales of Goods is expressly excluded. This Agreement and other Fortinet agreements may be amended or supplemented only by a writing that refers explicitly to the agreement signed on behalf of both parties, or, for this Agreement, as otherwise expressly provided in the lead-in above Section 1 above, provided, notwithstanding anything to the contrary and except for this Agreement which may be amended or updated as expressly provided in the lead-in above Section 1 above, for any amendment or other agree-

ment to be binding on Fortinet, such amendment or other agreement must be signed by Fortinet's General Counsel. No waiver will be implied from conduct or failure to enforce rights nor effective unless in a writing signed on behalf of the party against whom the waiver is asserted. If any part of this Agreement is found unenforceable, that part will be enforced to the maximum extent permitted and the remainder shall continue in full force and effect. You acknowledge that you have read this Agreement, understand it, and agree to be bound by its terms and conditions.

14. Privacy.

For information regarding Fortinet's collection, use and transfer of your personal information please read the Fortinet privacy policy on the Fortinet web site (<http://www.fortinet.com/aboutus/privacy.html>).

15. Open Source Software.

Fortinet's products may include software modules that are licensed (or sublicensed) to the user under the GNU General Public License, Version 2, of June 1991 ("GPL") or GNU Lesser General Public License, Version 2.1, of February 1999 ("LGPL") or other open source software licenses which, among other rights, permit the user to use, copy, modify and redistribute modules, or portions thereof, and may also require attribution disclosures and access to the source code ("Open Source Software"). The GPL requires that for any Open Source Software covered under the GPL, which is distributed to someone in an executable binary format, that the source code also be made available to those users. For any Open Source Software covered under the GPL, the source code is made available on this CD or download package. If any Open Source Software licenses require that Fortinet provide rights to use, copy or modify a Open Source Software program that are broader than the rights granted in this agreement, then such rights shall take precedence over the rights and restrictions herein. Fortinet will provide, for a charge reflecting our standard distribution costs, the complete machine-readable copy of the modified software modules. To obtain a complete machine-readable copy, please send your written request, along with a check in the amount of US \$25.00, to General Public License Source Code Request, Fortinet, Inc., 899 Kifer Rd, Sunnyvale, CA 94086 USA. In order to receive the modified software modules, you must also include the following information: (a) Name, (b) Address, (c) Telephone number, (d) E-mail Address, (e) Product purchased (if applicable), (f) Product Serial Number (if applicable). All open source software modules are licensed free of charge. There is no warranty for these modules, to the extent permitted by applicable law. The copyright holders provide these software modules "AS-IS" without warranty of any kind, either expressed or implied. In no event will the copyright holder for the open source software be liable to you for damages, including any special, incidental or consequential damages arising out of the use or inability to use the software modules, even if such holder has been advised of the possibility of such damages. A full copy of this license, including additional open source software license disclosures and third party license disclosures applicable to certain Fortinet products, may be obtained by contacting Fortinet's Legal Department at legal@fortinet.com.

GNU GENERAL PUBLIC LICENSE GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.

59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you". Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the

Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program. You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if

the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.) These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.. Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program. In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

Source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable. If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under

this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

GNU LESSER GENERAL PUBLIC LICENSE

Version 2.1, February 1999

Copyright (C) 1991, 1999 Free Software Foundation, Inc.

59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library. You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

- a) The modified work must itself be a software library.
- b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.
- c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.
- d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it. Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library. In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2 instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy. This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not.

Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.) Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for your own use and reverse engineering for debugging such modifications. You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of

definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

b) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.

c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy. For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable. It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this

License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice. This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. Each version is

given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

15. The warranty disclaimer contained in Sections 11 and 12 of the preceding GPL License is incorporated herein.

About This Guide

This preface includes the following sections:

- Audience
- Purpose

Audience

This guide is for network administrators who are implementing FortiConnect to manage secure User and Device connectivity on their networks. FortiConnect works alongside Wireless Controllers, LAN Switches, NAC Systems, Firewalls and other Network Enforcement devices which provide the captive portal and enforcement point for User connectivity and Smart Connect functionality for onboarding devices.

Purpose

The FortiConnect Installation and Configuration Guide describes how to install and configure the FortiConnect appliance. It describes the simple initial installation of the appliance via CLI and the configuration and administration of the FortiConnect Portal through the web-based interface.

Purpose

Welcome to FortiConnect

FortiConnect is a complete provisioning, management, and reporting system that provides temporary network access for guests, visitors, contractors, consultants, or customers. FortiConnect works alongside Wireless Controllers, LAN Switches, NAC Systems, Firewalls and other Network Enforcement devices which provide the captive portal and enforcement point for User access.

FortiConnect allows any user with privileges to easily create temporary User accounts and sponsor those users for network access. FortiConnect performs full authentication of sponsors, the users who create accounts, and allows sponsors to provide account details to the User by printout, email, or SMS. The entire experience, from user account creation to network access, is stored for audit and reporting.

When User accounts are created, they are stored within the built-in database on the FortiConnect server. When using FortiConnect's built-in database, external network access devices, such as the Wireless LAN Controller, can authenticate users against FortiConnect using the RADIUS (Remote Authentication Dial In User Service) protocol.

FortiConnect provisions the User account for the amount of time specified when the account is created. Upon expiry of the account, FortiConnect either deletes the account or sends a RADIUS message which notifies the controller of the amount of valid time remaining for the account before the controller should remove the user.

FortiConnect provides vital network access accounting by consolidating the entire audit trail from account creation to actual use of the account so that reports can be performed through a central management interface.

FortiConnect Concepts

FortiConnect makes use of a number of terms to explain the components needed to provide User access.

The Guest/User

The Guest/User is the person who needs an account to access the network. A Guest or a User normally accesses the network using their own device, connecting to a wired or wireless hotspot provided by an organization. They normally have their browser connection redirected to a portal where they can login by the Network Enforcement Device. Throughout the documentation you will see references to a Guest or a User whereas these are essentially the same person.

Sponsor

The sponsor user is the person who creates the User account. This person is often an employee of the organization that provides the network access. Sponsors can be specific individuals with certain job roles, or can be any employee who can authenticate against a corporate directory such as Microsoft Active Directory (AD).

Admin

The admin user is the administrator who configures and maintains the FortiConnect appliance.

Network Enforcement Device

These devices are the network infrastructure components that provide the network access. Additionally, network enforcement devices are responsible for pushing Users to a captive portal where they can enter their account details. The captive portal can sit on either the Network Enforcement Device, or FortiConnect. When a User enters his or her temporary user name and password, the network enforcement device checks those credentials against the accounts created by the FortiConnect.

FortiConnect

FortiConnect ties together all the pieces of User access. FortiConnect links the sponsor creating the account, the account details passed to the User, the User authentication against the network enforcement device, and the network enforcement device's verification of the User with the FortiConnect. Additionally, FortiConnect consolidates accounting information from network enforcement devices to provide a single point of User access reporting from who created the account, to when the User accessed the network and exactly what they did while on the network.

Installing FortiConnect

FortiConnect is supported on the following platforms:

- VMware virtual machine
- Microsoft Hyper-V
- SA200, SA250 and SA2000

The following sections walk you through installing FortiConnect on each of these platforms using the FortiConnect ISO image available in the download section of the Support Portal.

Note: PLEASE NOTE THAT FortiConnect 14.10 CAN ONLY BE UPGRADED FROM FortiConnect RELEASES 13.10 and 14.2

Installing FortiConnect on VMware

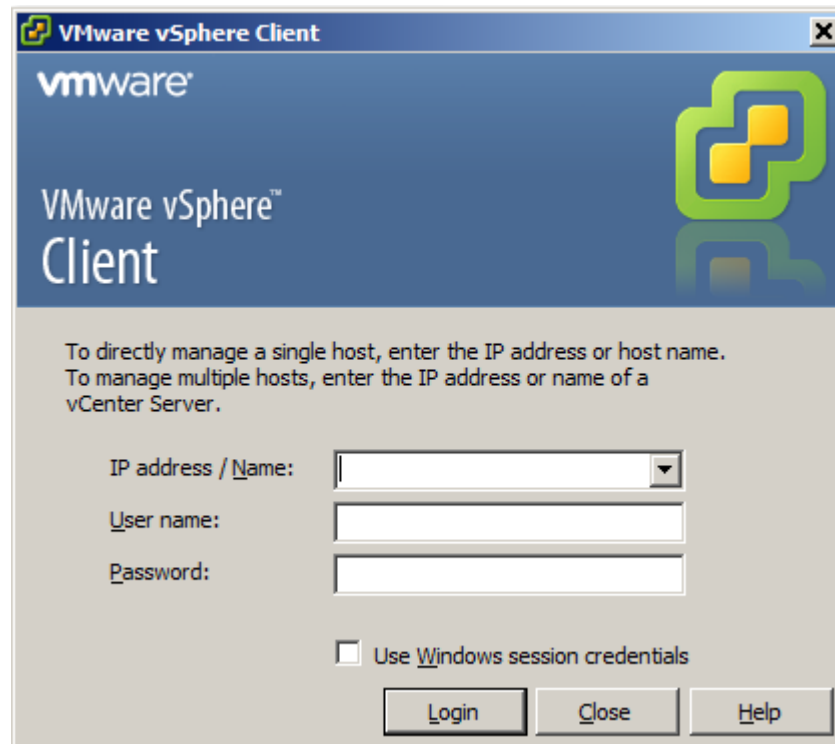
FortiConnect can be installed into a VMware virtual machine. The following platforms are supported for install

- ESX 3.5
- ESX 3.5i
- ESX 4.x
- ESX 4.xi
- ESX 5.xi
- Workstation 5.0 or later (only supported for evaluation and demonstration purposes only)
- Server 1.0 or later
- Fusion 2.0 or later (only supported for evaluation and demonstration purposes only)
- Microsoft Hyper V on Windows 2008 or later

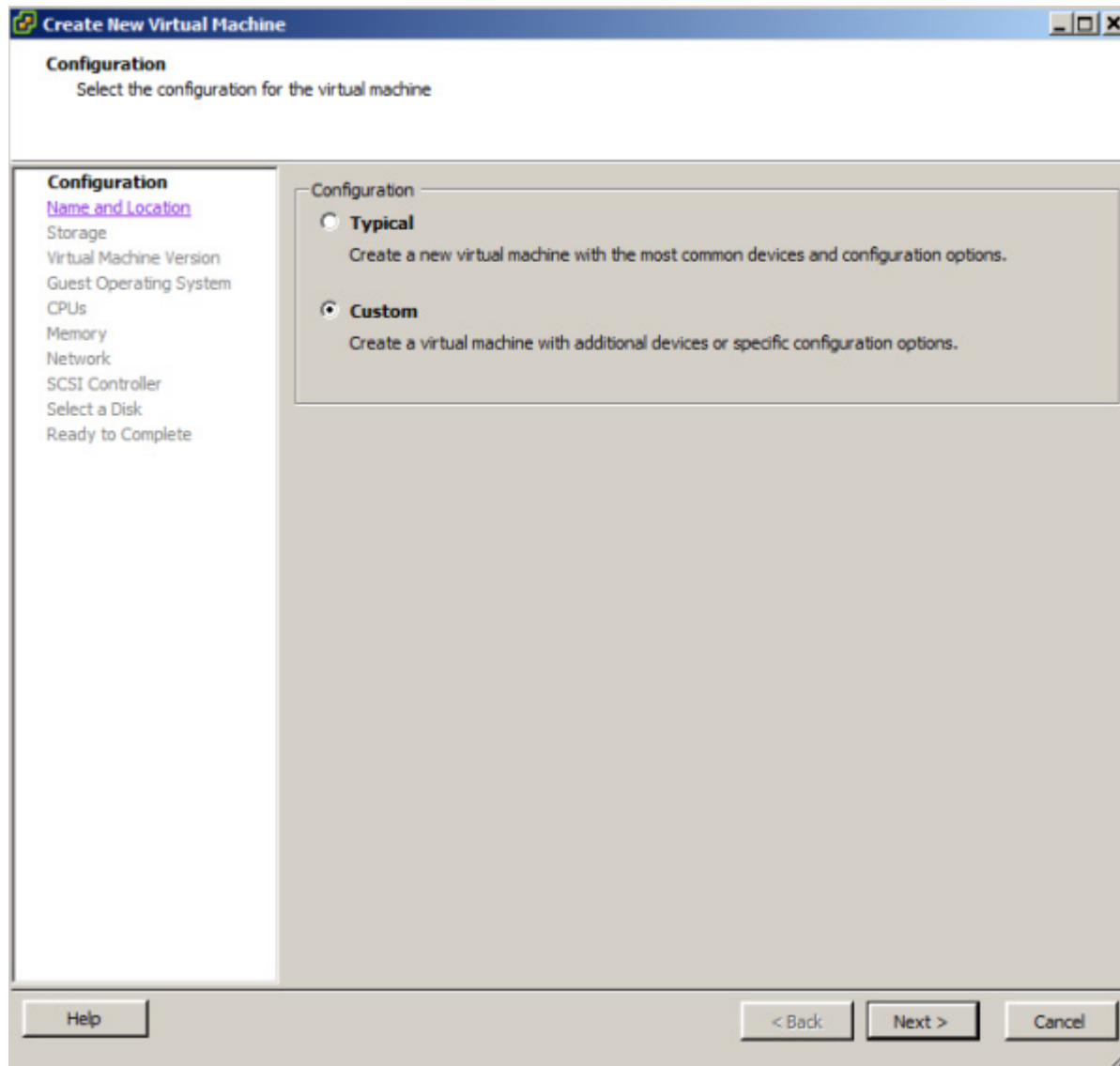
Note: Install steps are for VMware ESX 4.0 update 1. Installation steps on other VMware platforms may differ slightly but the general settings for the virtual machine should be followed.

Note: Don't use the 'easy install' option in VMware Workstation, please select 'custom install'

1. Login to your ESX server using the vSphere client.



2. Using the vSphere client copy the FortiConnect ISO file to a Datastore on the Host VMware Server.
3. From the drop down menus on the vSphere client go File -> New -> Virtual Machine.
4. From here, select Custom to customize the build and click on Next >.



5. Name the virtual machine appropriately and click on Next.

The screenshot shows the 'Create New Virtual Machine' wizard in VMware Workstation. The window title is 'Create New Virtual Machine'. The current step is 'Name and Location', with the instruction 'Specify a name and location for this virtual machine'. The 'Virtual Machine Version' is set to 8. On the left, a navigation pane lists the steps: Configuration (highlighted), Name and Location (current), Storage, Guest Operating System, Network, Create a Disk, and Ready to Complete. The main area shows a 'Name:' field with the text 'Identity Manager 14.2.0'. Below the field, there is explanatory text: 'Virtual machine (VM) names may contain up to 80 characters and they must be unique within each vCenter Server VM folder.' and 'VM folders are not viewable when connected directly to a host. To view VM folders and specify a location for this VM, connect to the vCenter Server.' At the bottom, there are buttons for 'Help', '< Back', 'Next >', and 'Cancel'.

Create New Virtual Machine

Name and Location
Specify a name and location for this virtual machine

Virtual Machine Version: 8

Configuration
Name and Location
Storage
Guest Operating System
Network
Create a Disk
Ready to Complete

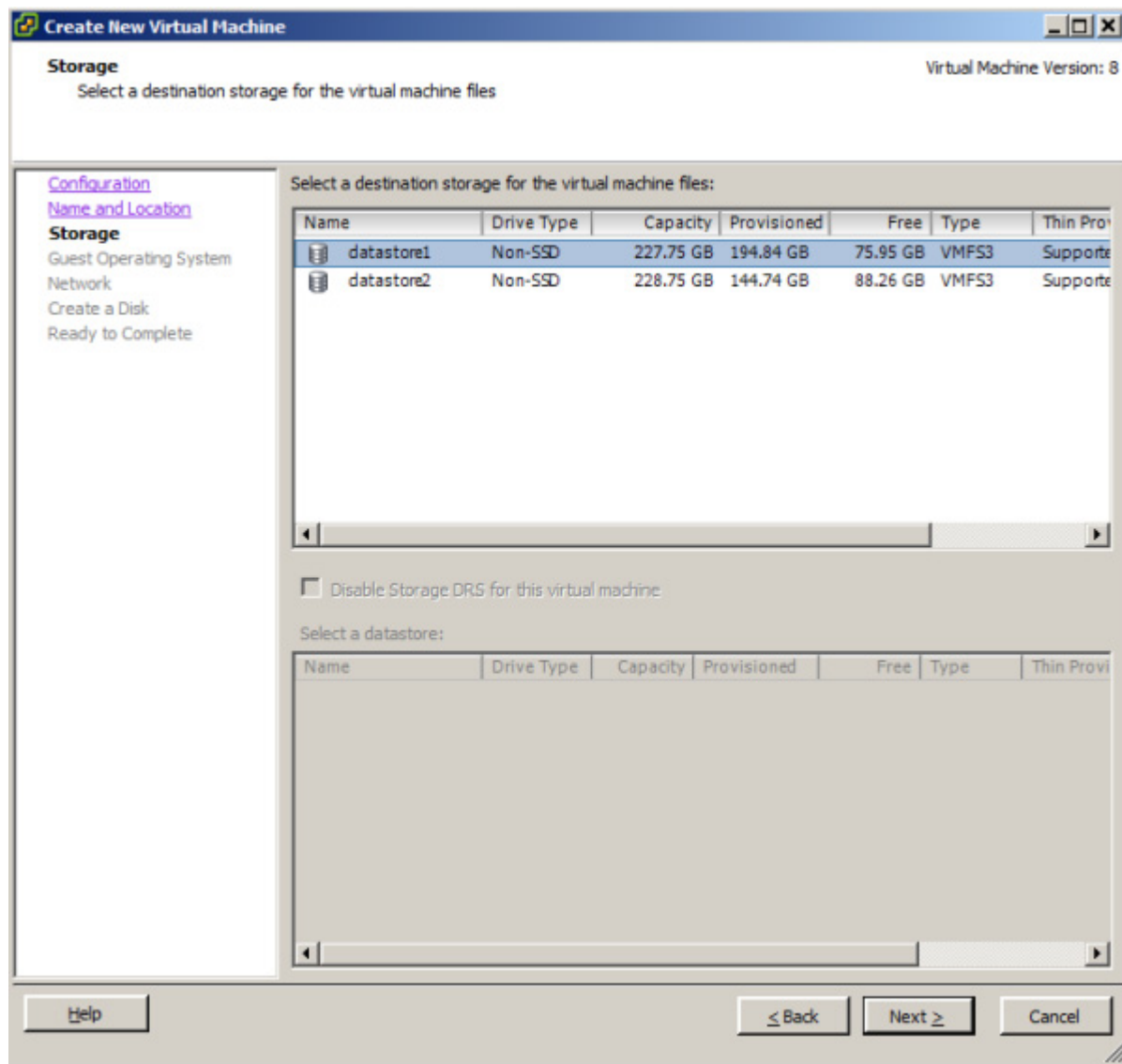
Name:
Identity Manager 14.2.0

Virtual machine (VM) names may contain up to 80 characters and they must be unique within each vCenter Server VM folder.

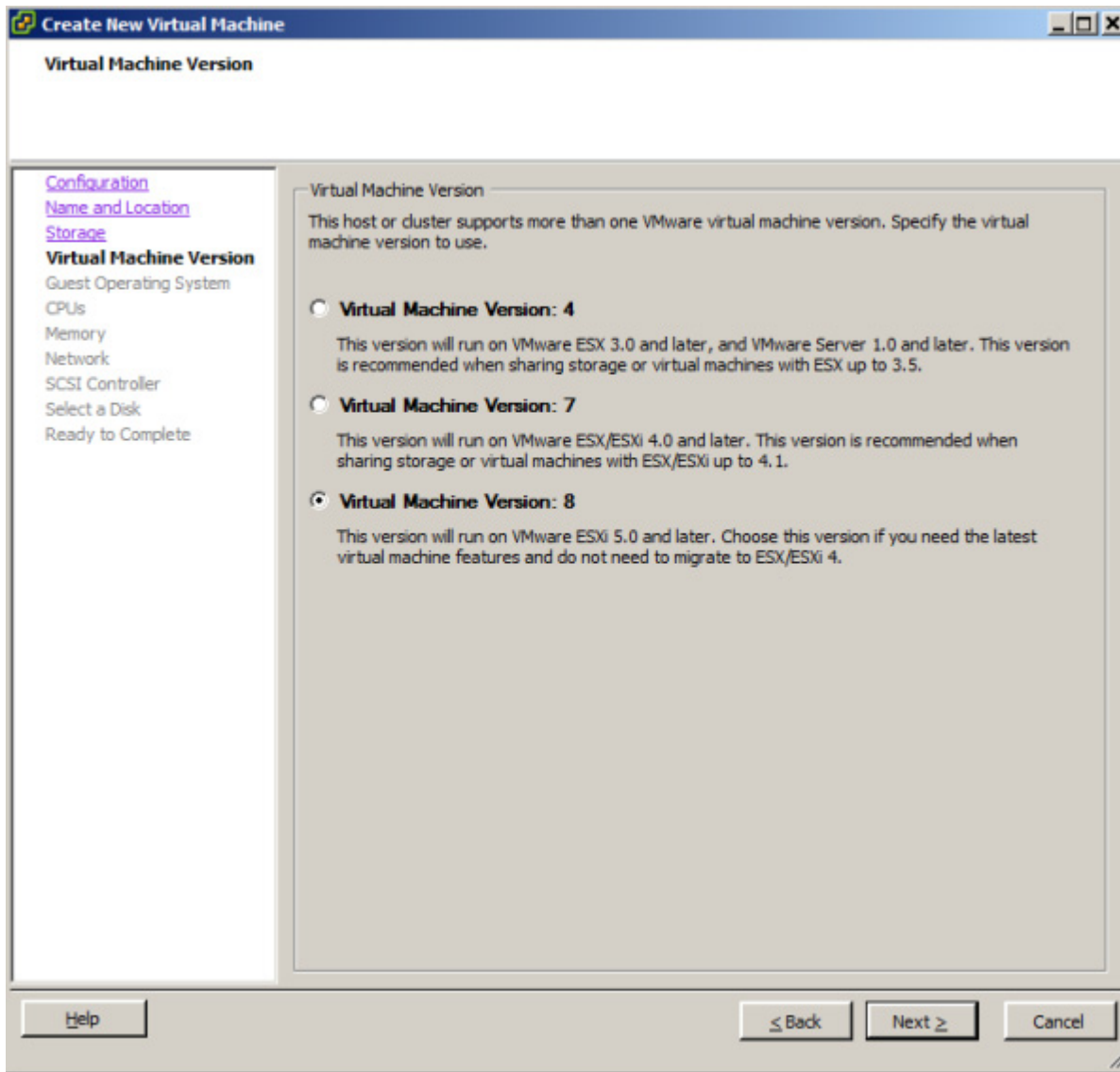
VM folders are not viewable when connected directly to a host. To view VM folders and specify a location for this VM, connect to the vCenter Server.

Help < Back Next > Cancel

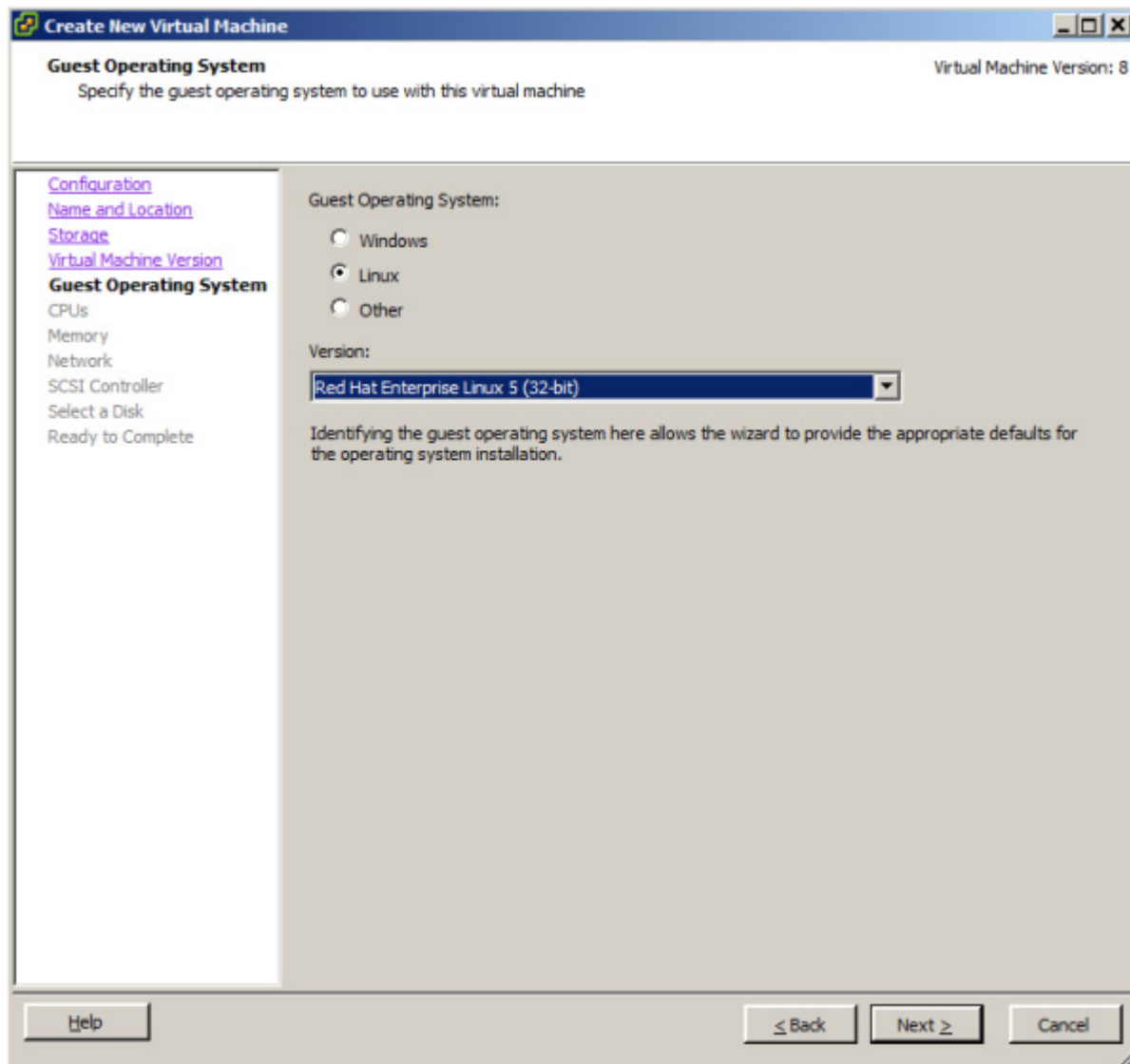
6. Select a Datastore to install to and click on Next.



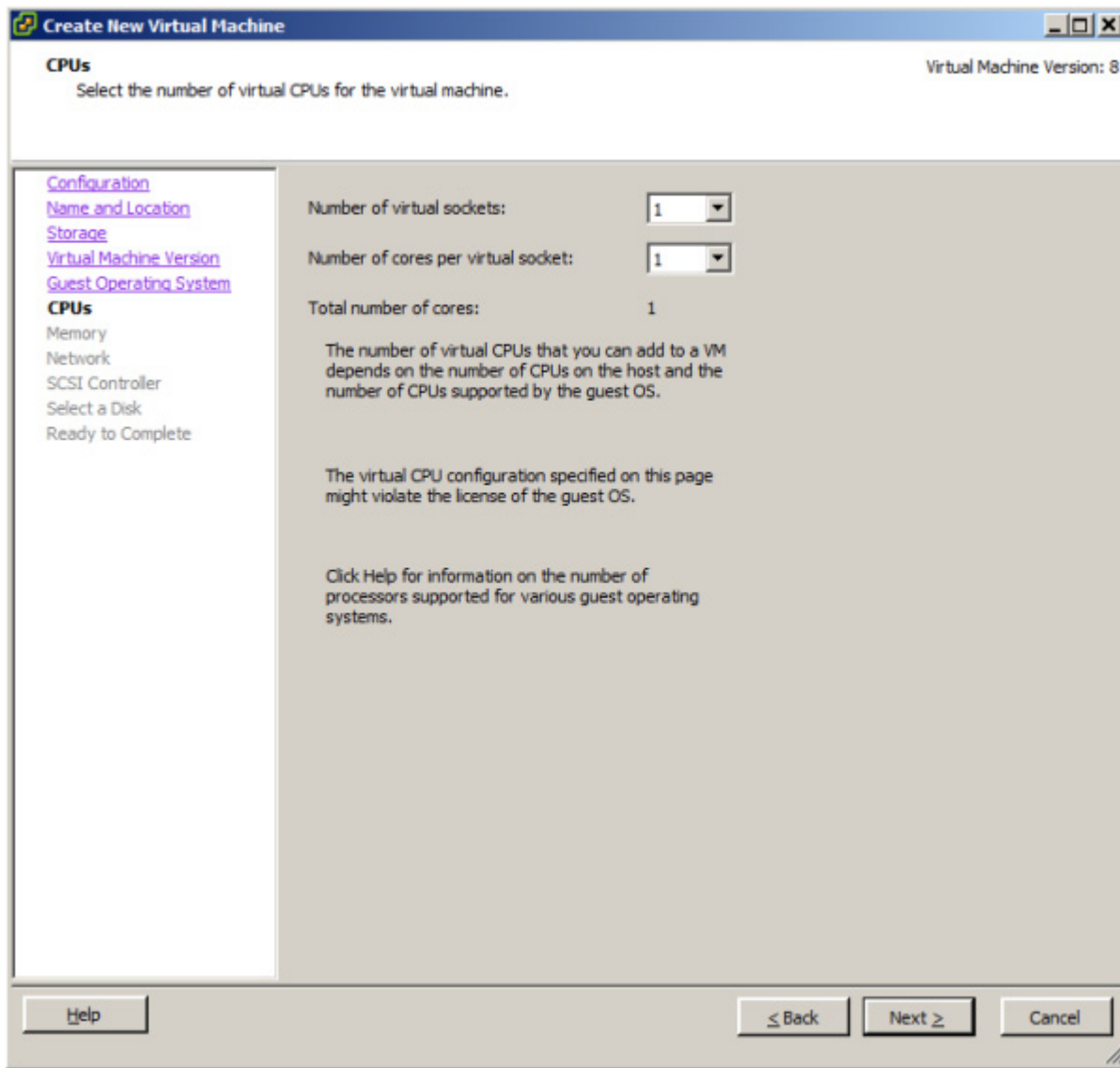
7. Select Virtual Machine Version 8 and click on Next.



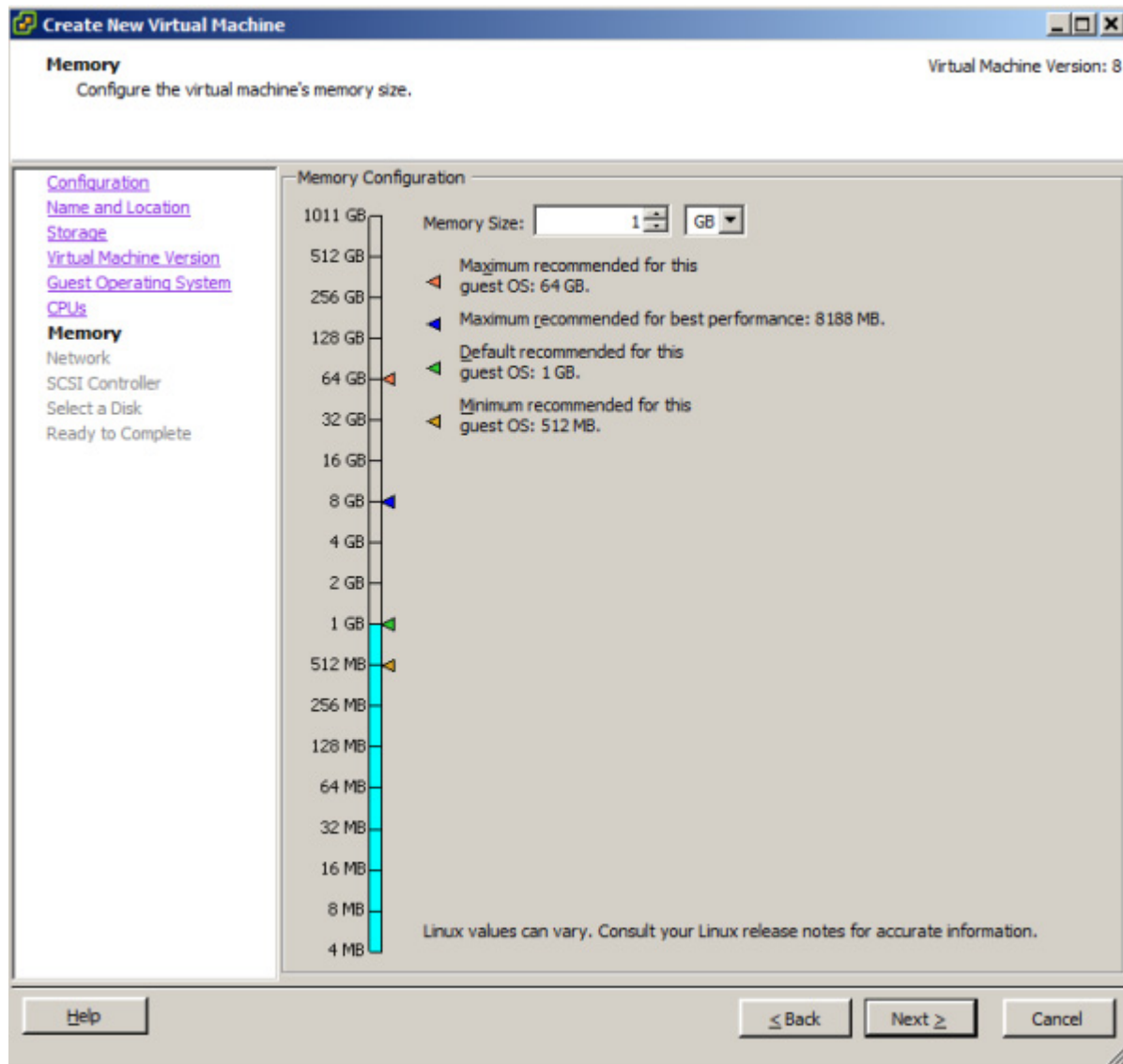
8. Select Linux - Red Hat Enterprise Linux 5 (32-bit) and click on Next.



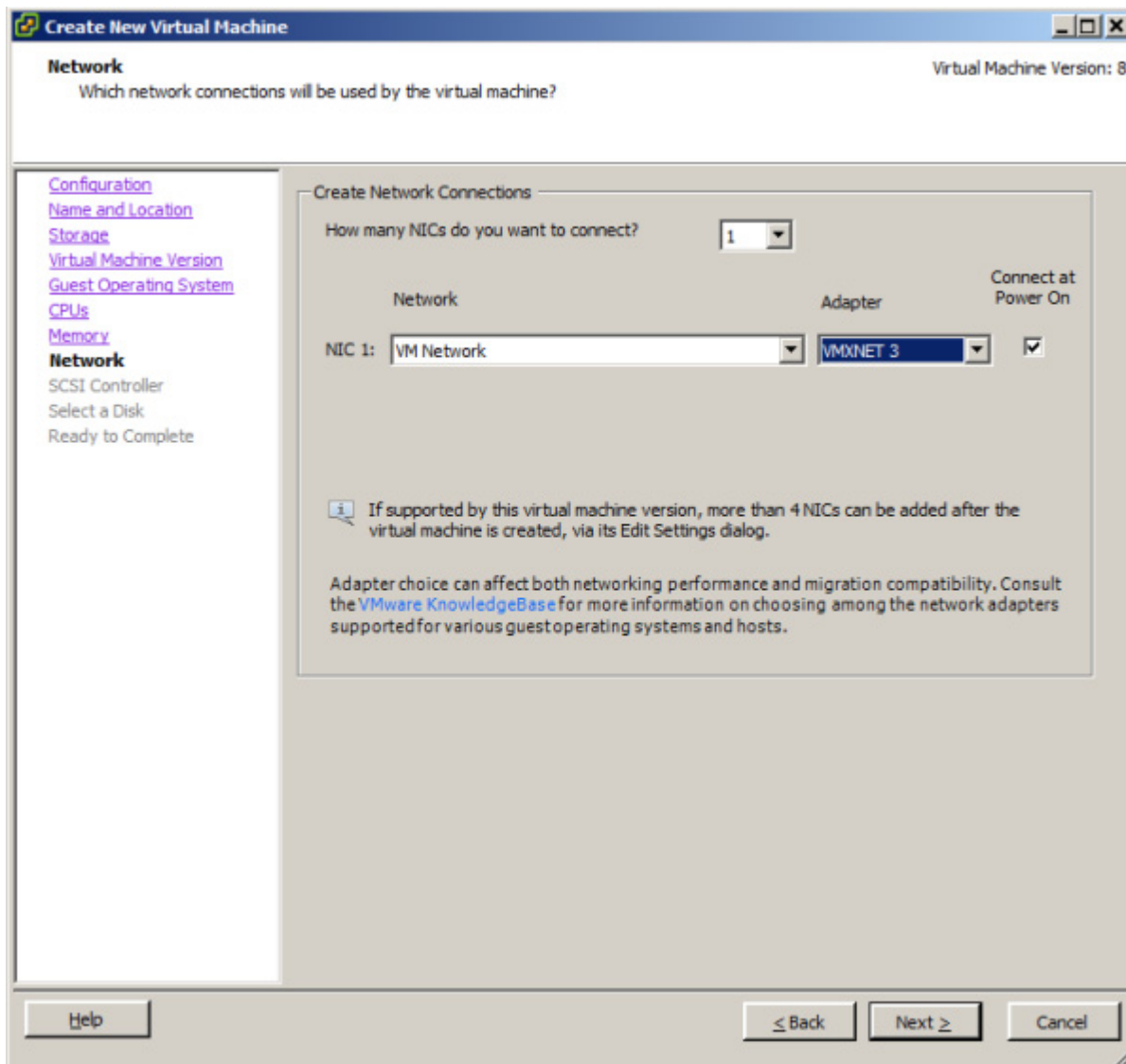
9. Choose 2 for the amount of Virtual Cores and click on Next.



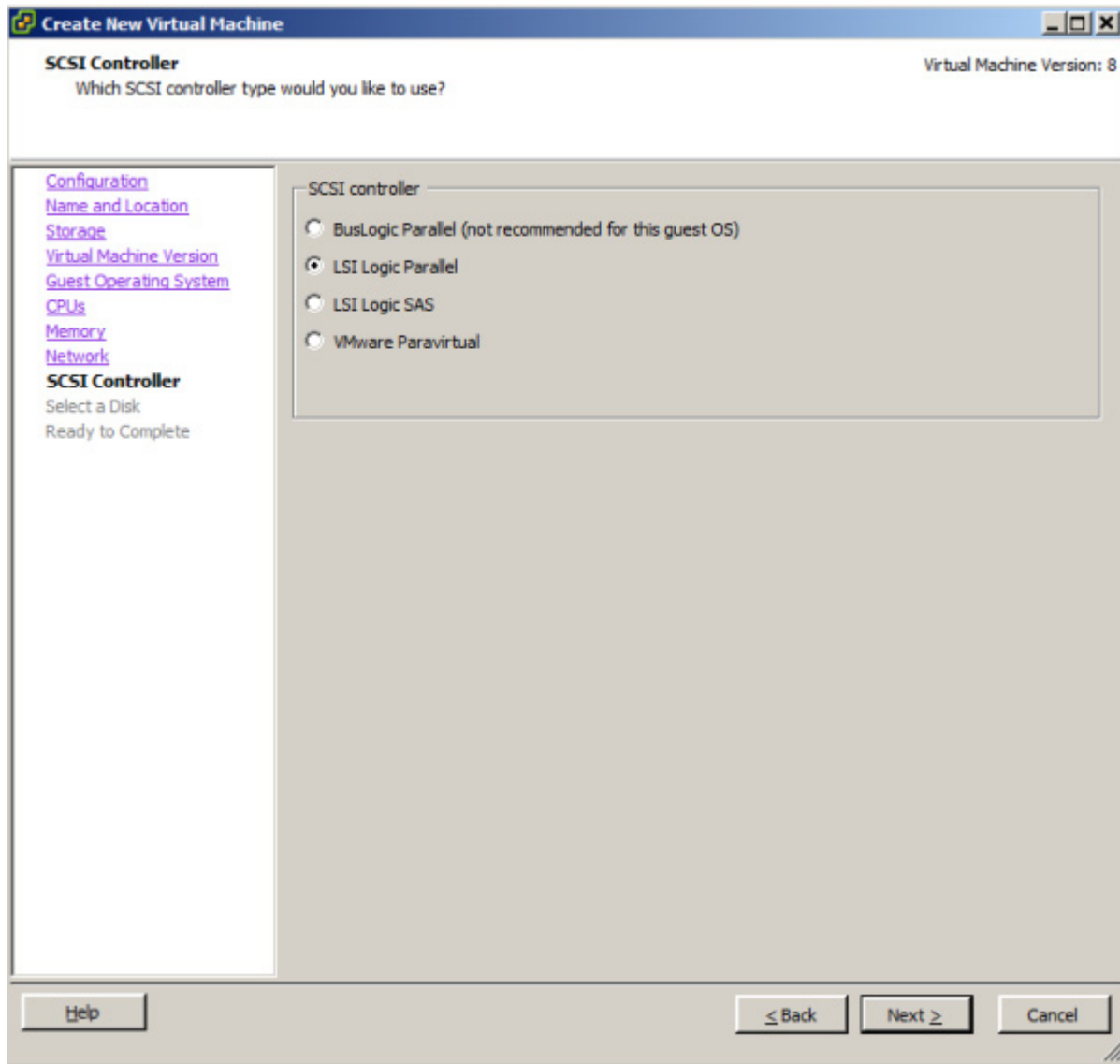
10. Select a Memory Size of a minimum 4Gb.



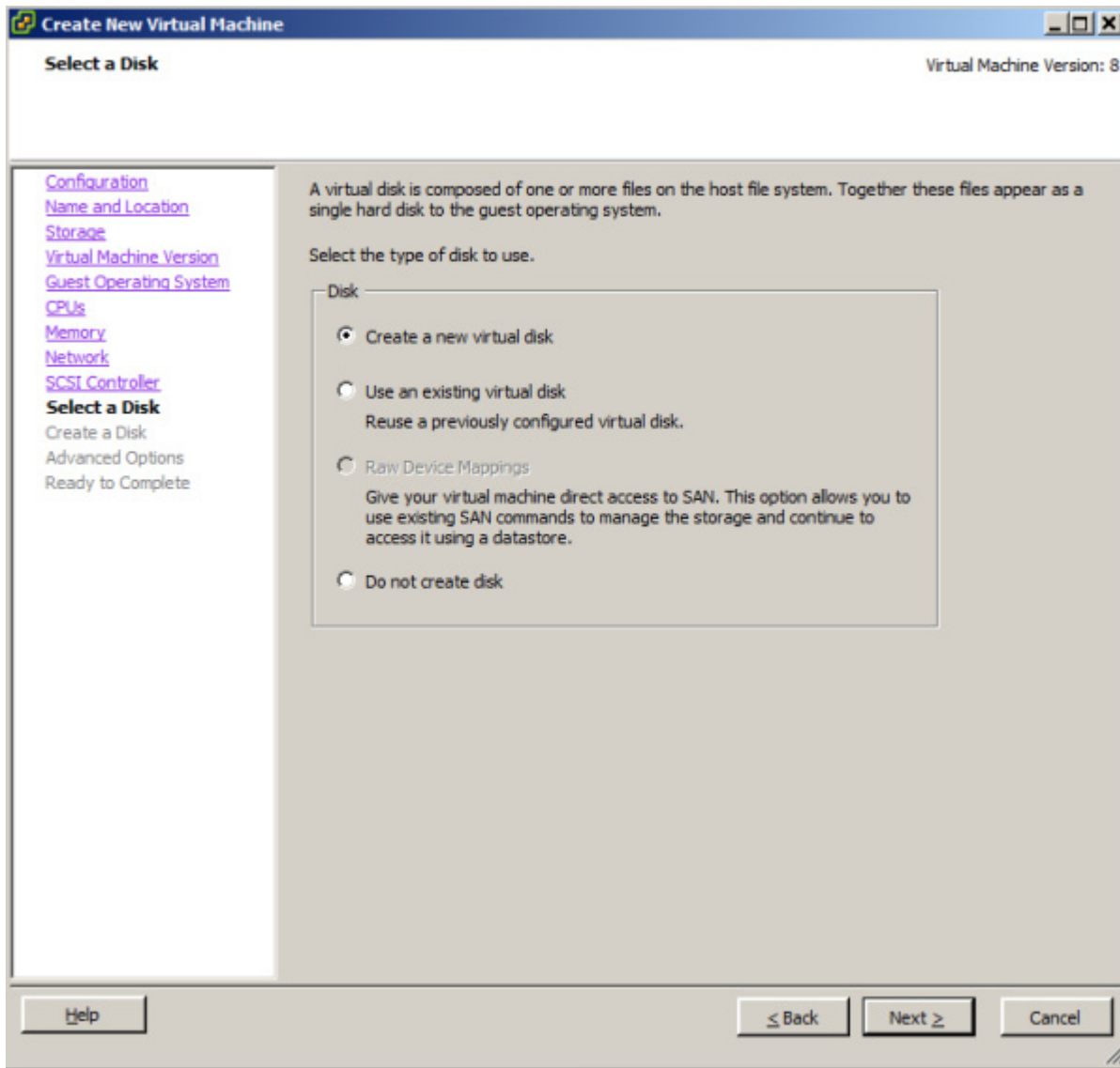
11. Choose to Connect 1 NIC (Choose adapter VMXNET 3 from the drop down menu) and then click on Next.



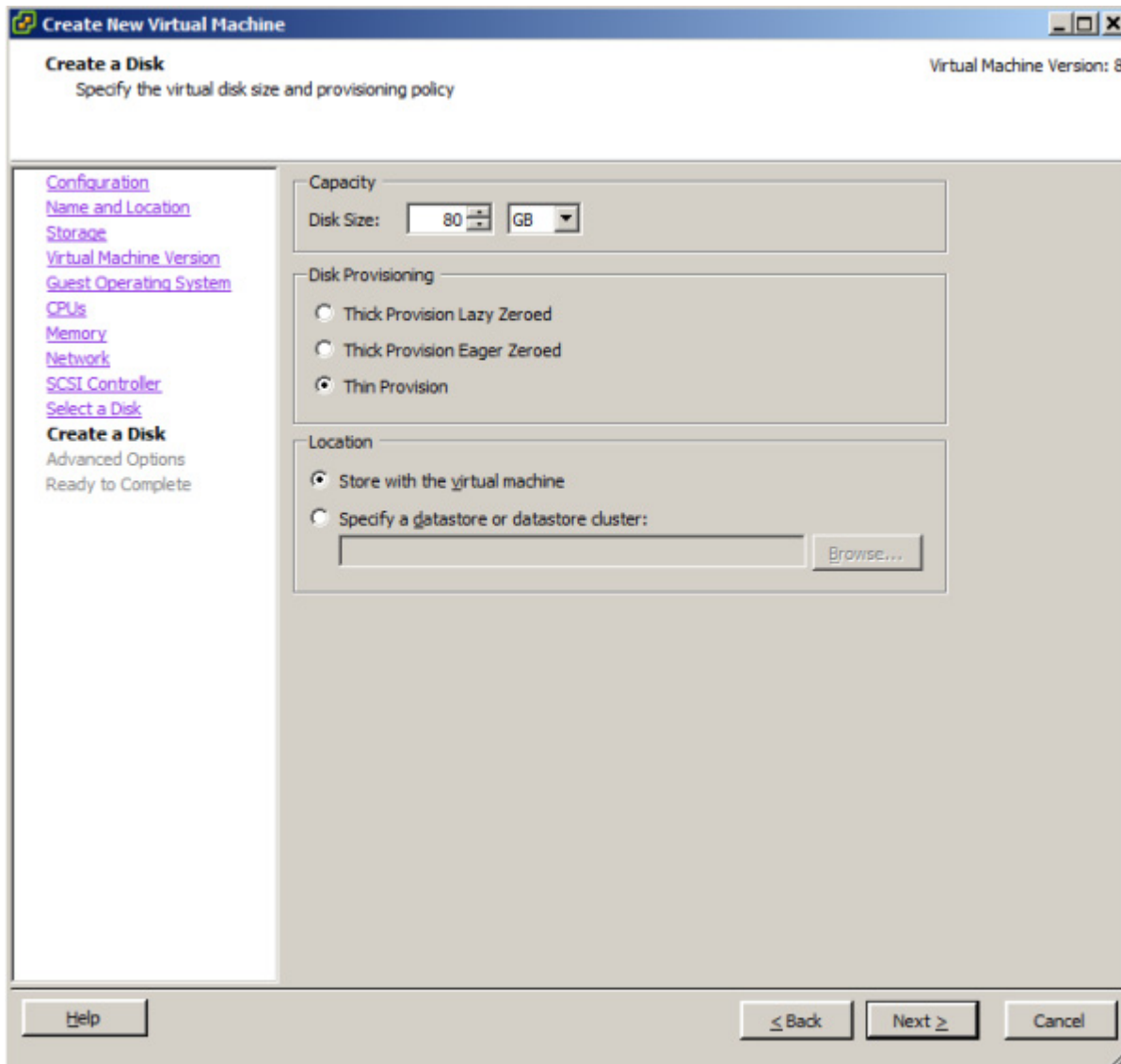
12. Leave the SCSI controller as default then click on Next.



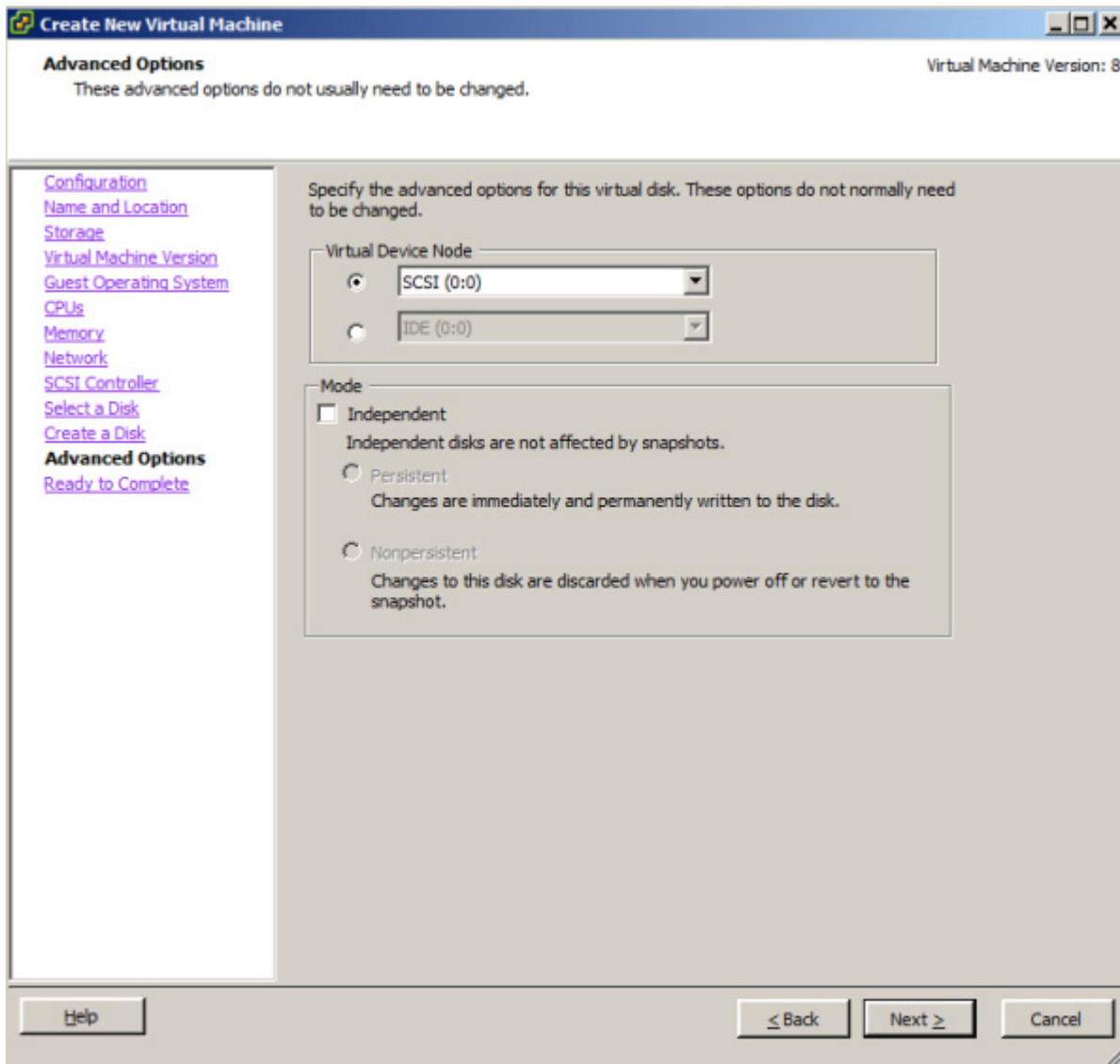
13. Select Create new virtual disk and click on Next.



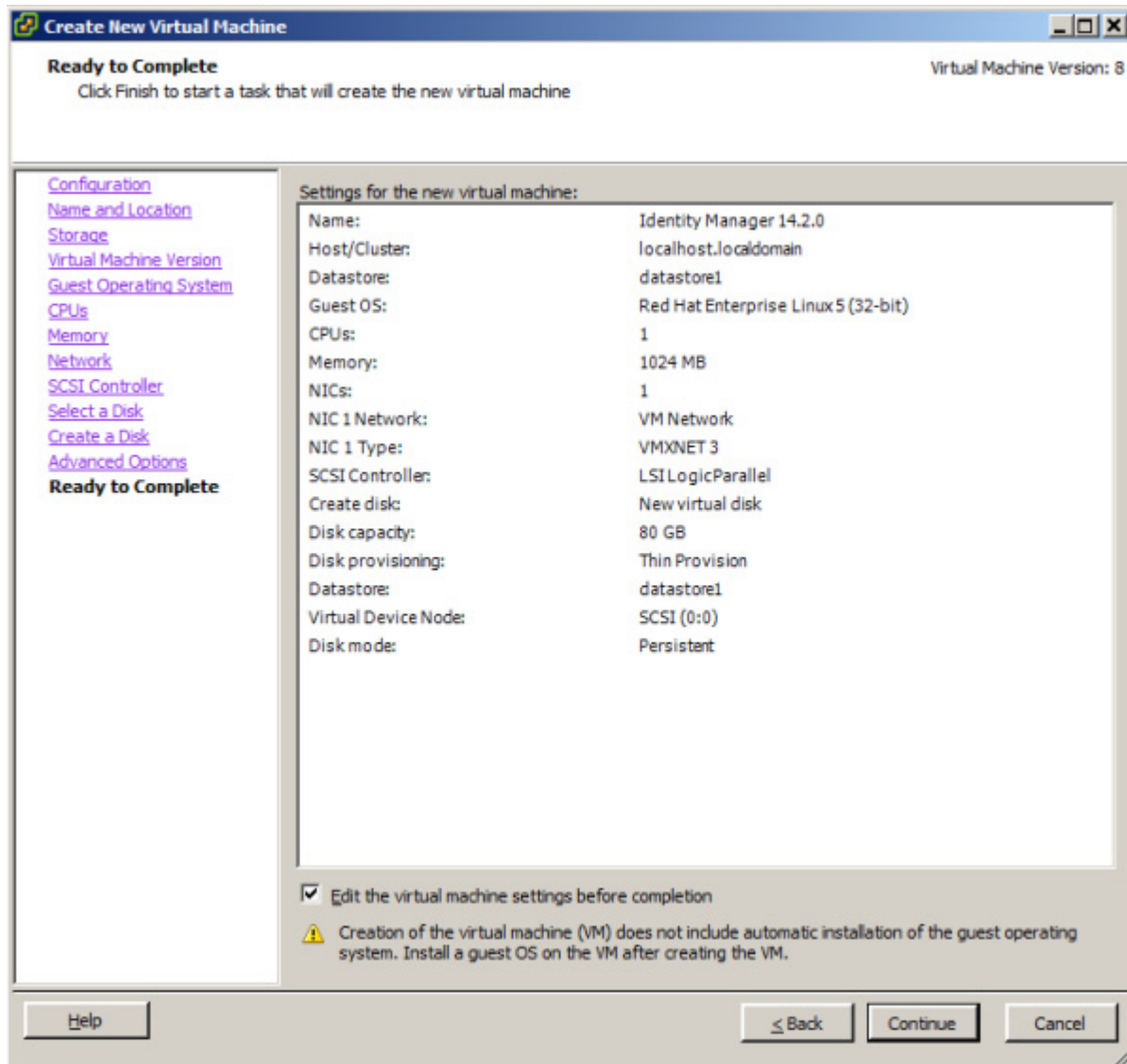
14. Choose a Disk size with a minimum of 50Gb (test and lab environments), minimum 100Gb for live environments (thin provisioning recommended where necessary) and select Store with the virtual machine and click on Next. Thin provisioning may be selected, however this does have a performance penalty.



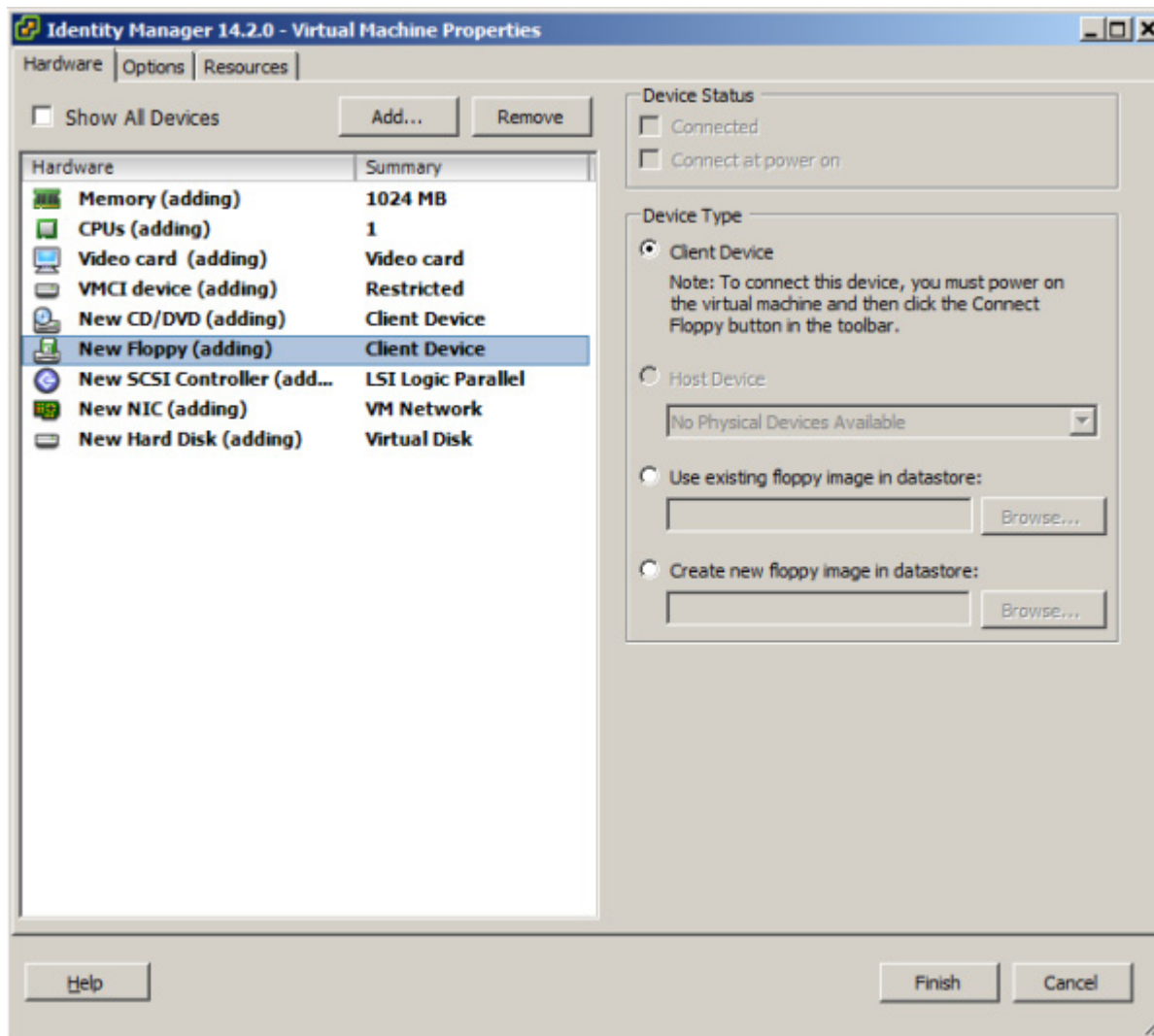
15. Select the Virtual device node to be SCSI (0:0) and click on Next.



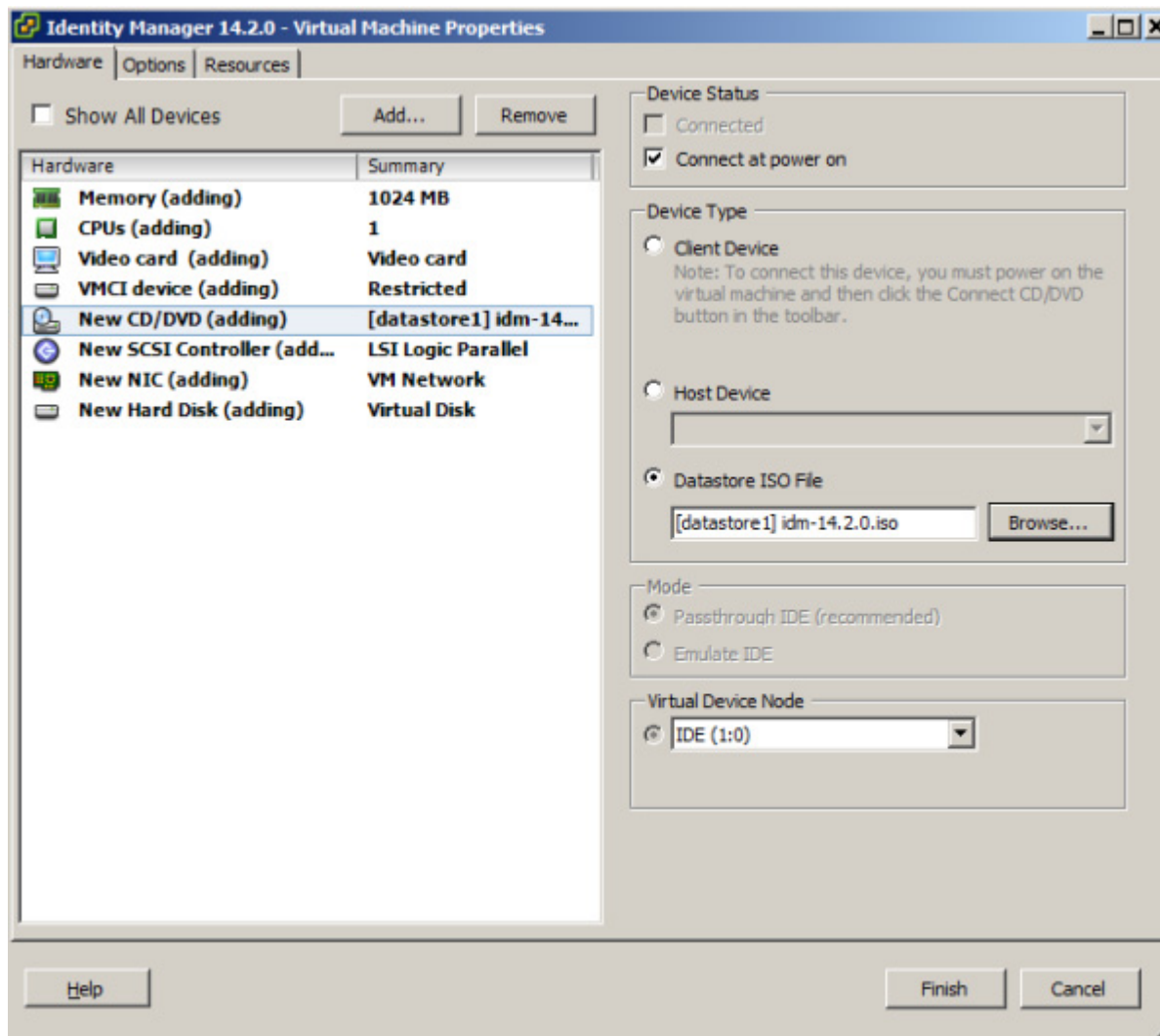
16. Select the Edit The Virtual Machine before completion and click on Continue.



17. Remove the floppy device by selecting the New Floppy on the hardware list and click on Remove.



18. Set CD/DVD to the datastore ISO file you uploaded in Step 1 by selecting the New CD/DVD on the hardware list, and on the right hand menu select Datastore ISO and browse to the file. Once chosen, click on Connect at power on.



19. Right click and select power on to power up your virtual machine.
20. Go to the console tab.
21. At the boot prompt type "vmware" and hit enter.

```
-----
Welcome to the Meru Connect 14.10.0 Installation Process
-----

To install on a SA200 appliance type 'sa200' then press <ENTER>.
To install on a SA250 appliance type 'sa250' then press <ENTER>.
To install on a SA2000 appliance type 'sa2000' then press <ENTER>.
To install as a VMware guest type 'vmware' then press <ENTER>.
To install as as Hyper-V guest type 'hyper-v' then press <ENTER>.

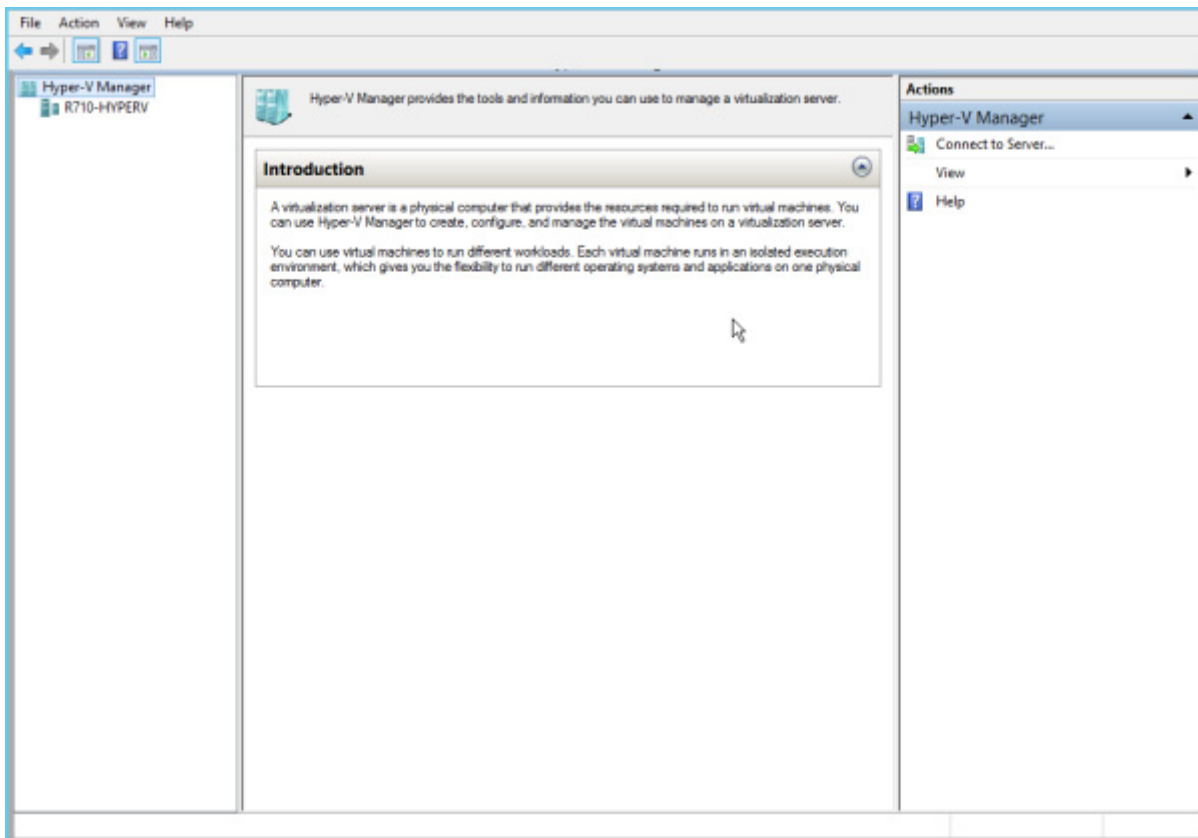
***** WARNING *****
This will remove all existing information from the hard disks in the computer.
Please make sure there is nothing that you need from the hard disk before
proceeding. There is no way of retrieving data after this process has run.
*****
boot: _
```

22. The install can take around 5-10 minutes and may appear to pause at times. When the login prompt appears installation is complete.

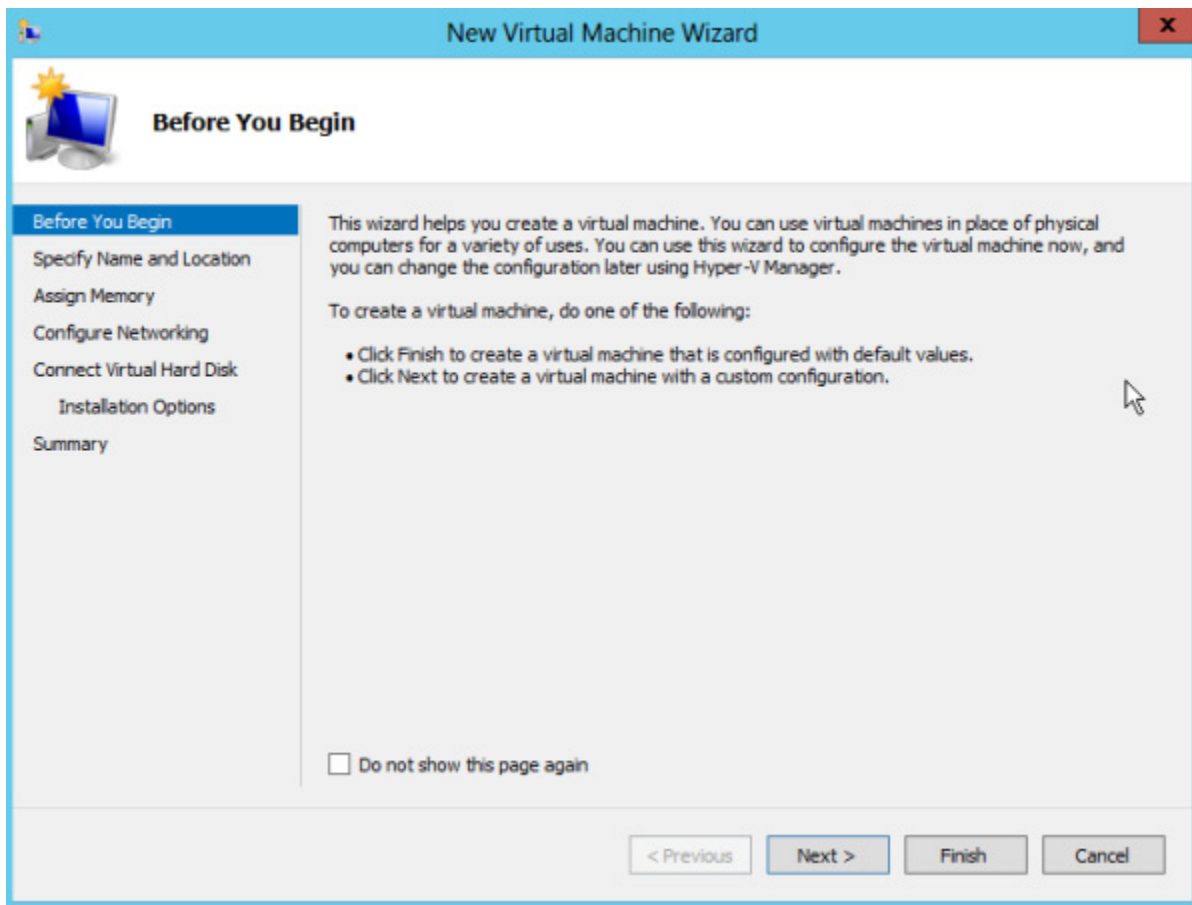
Installing on Microsoft Hyper-V

FortiConnect can be installed on Microsoft Hyper-V.

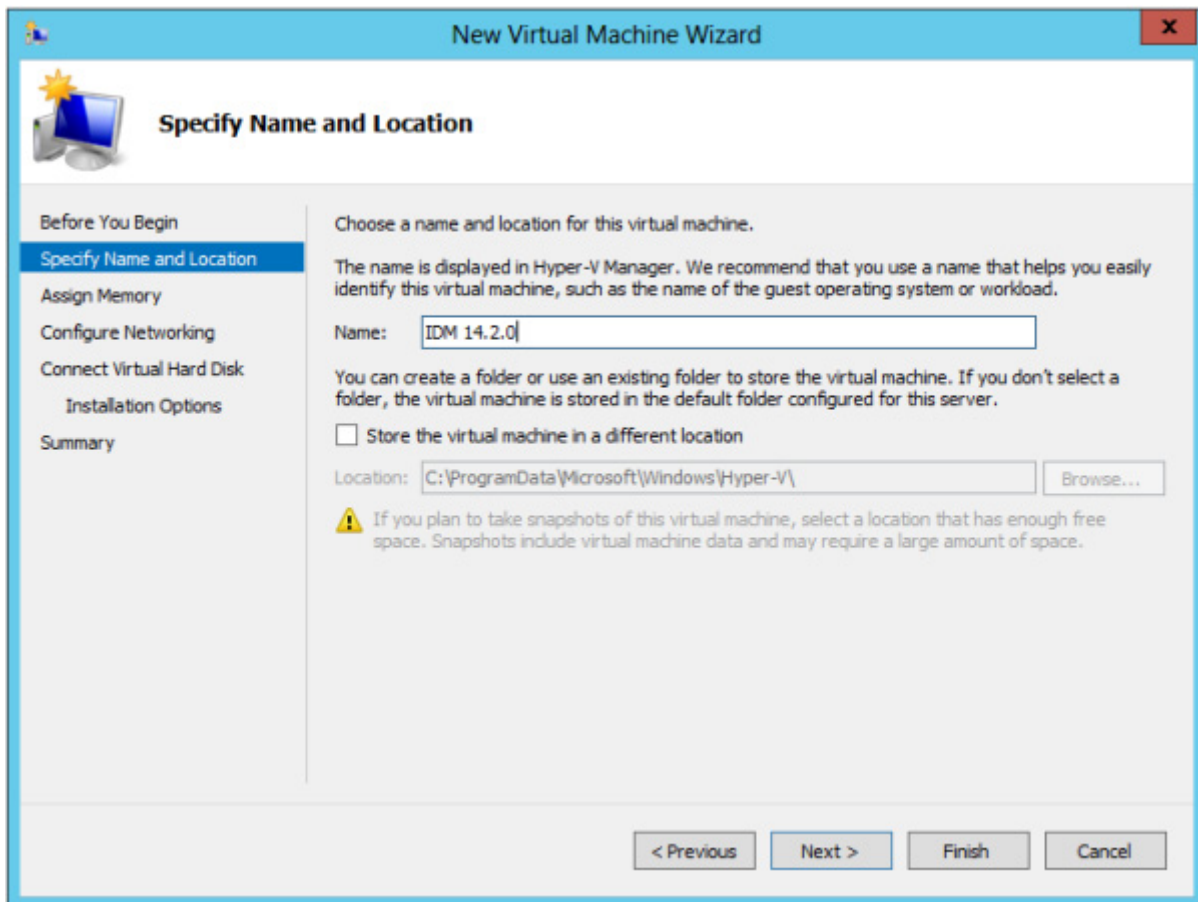
1. Open up Hyper-V manager as shown in the screenshot below



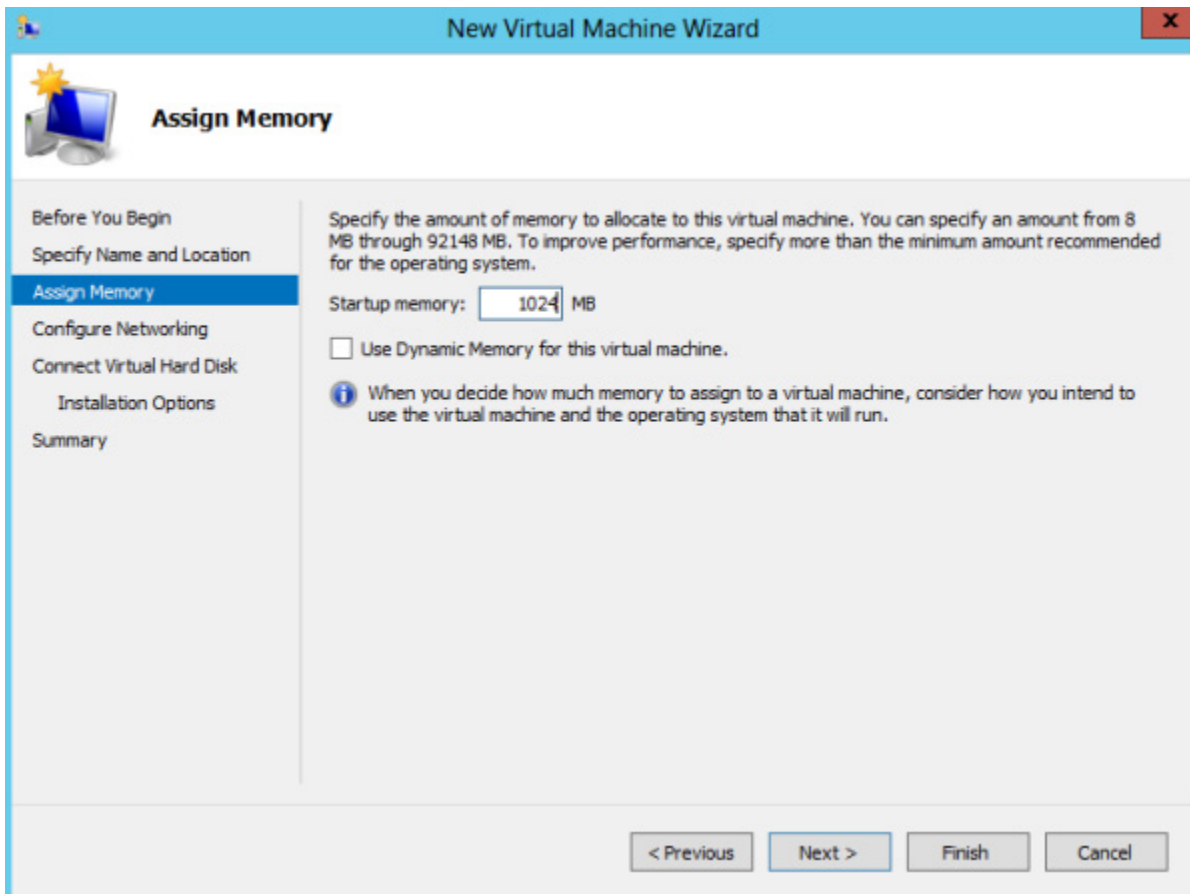
2. To bring up the New Virtual Machine Wizard, click on New underneath the Actions column and select virtual machine.



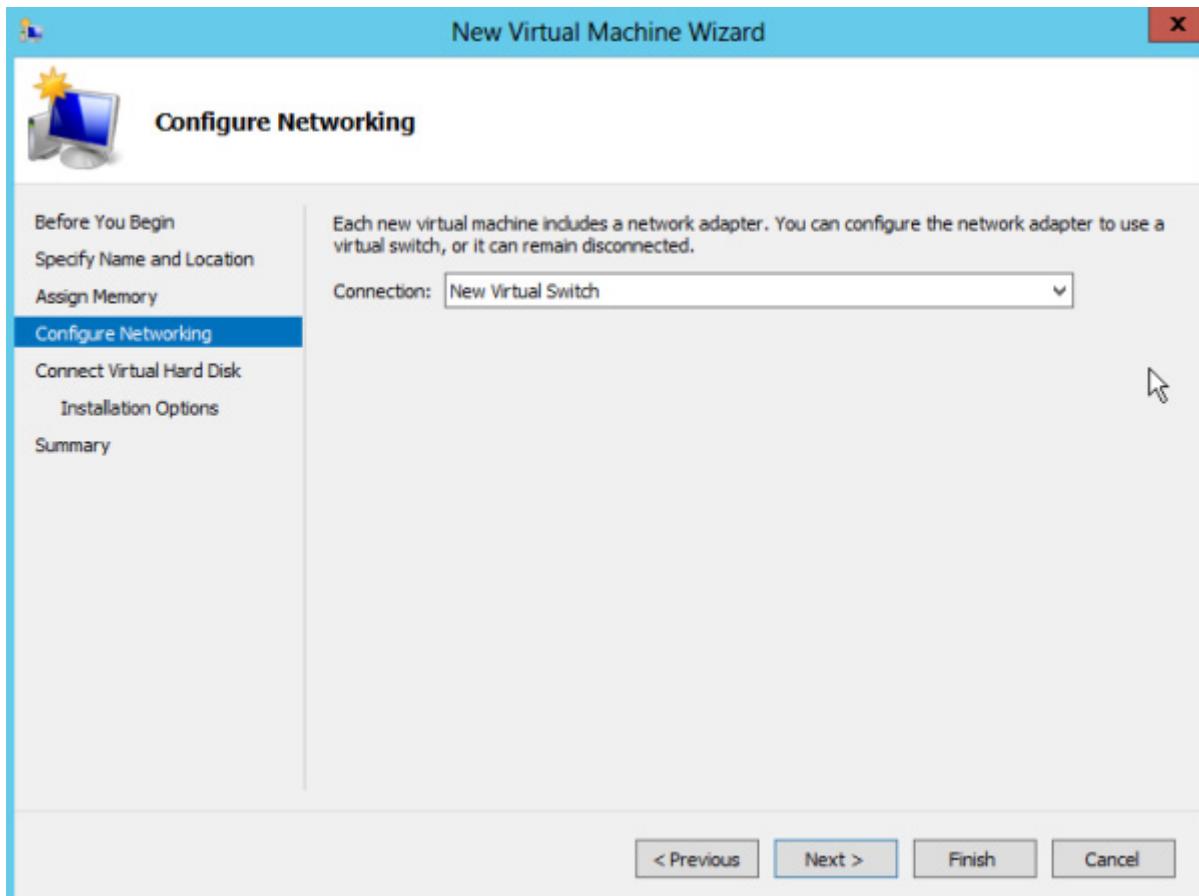
3. Click on Next to create a virtual machine with a custom configuration.



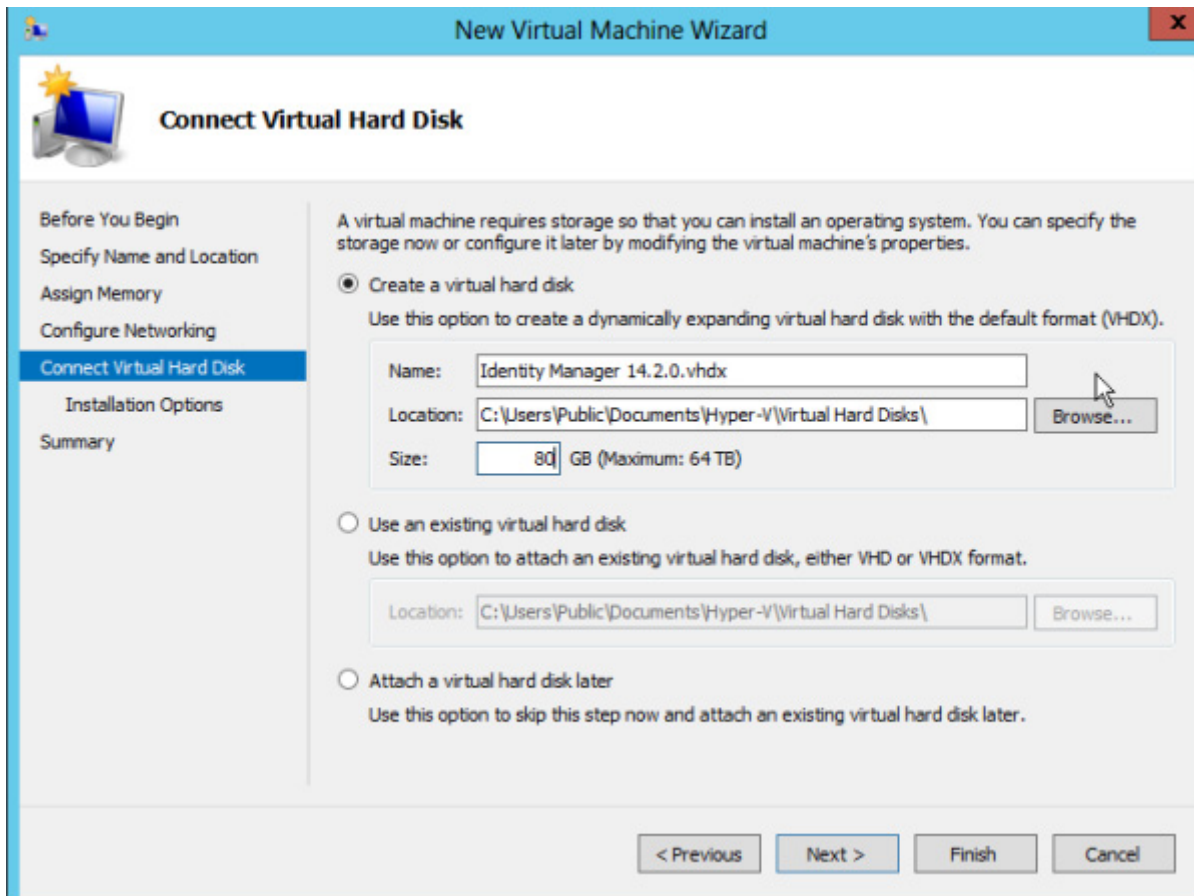
4. Choose a name and location for the virtual machine and then click on Next.



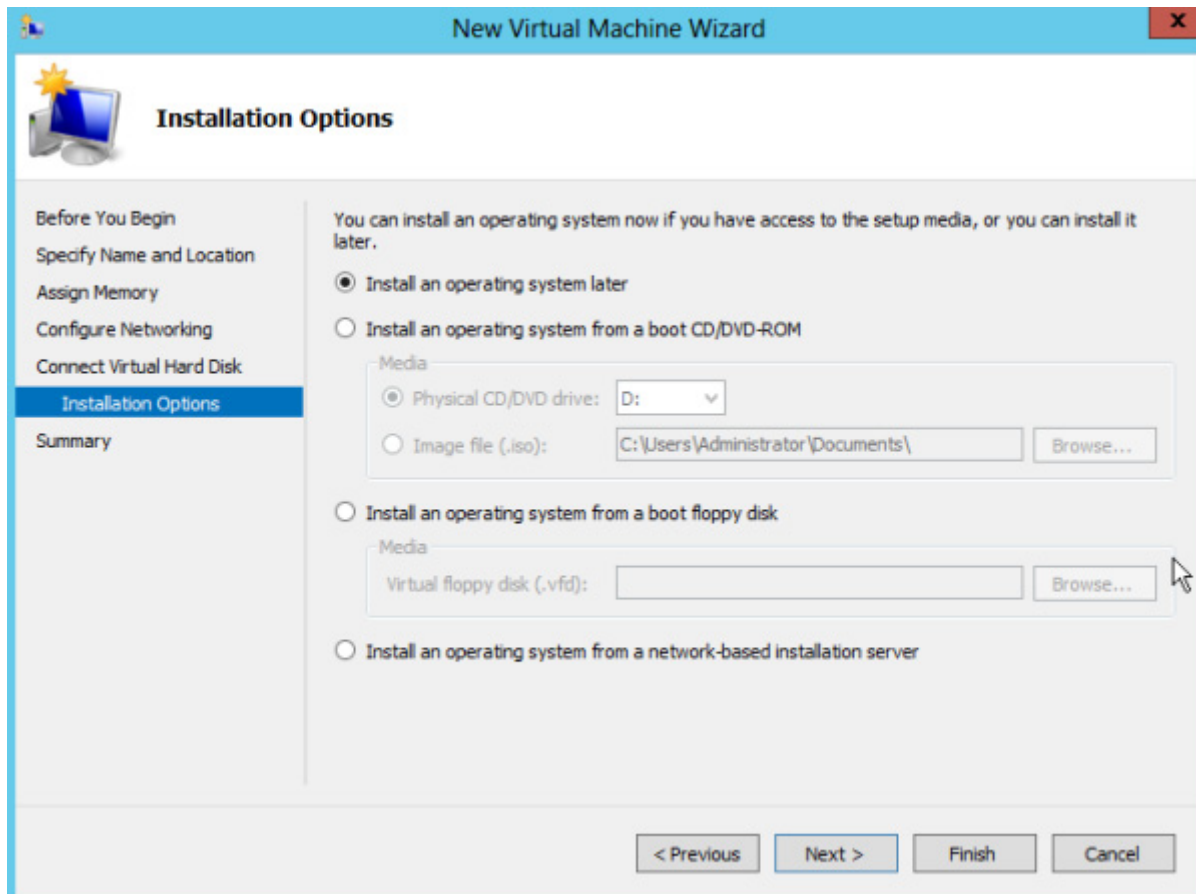
5. Select the amount of memory you wish to allocate to your virtual machine, a minimum of 4GB is recommended, and then click on Next.



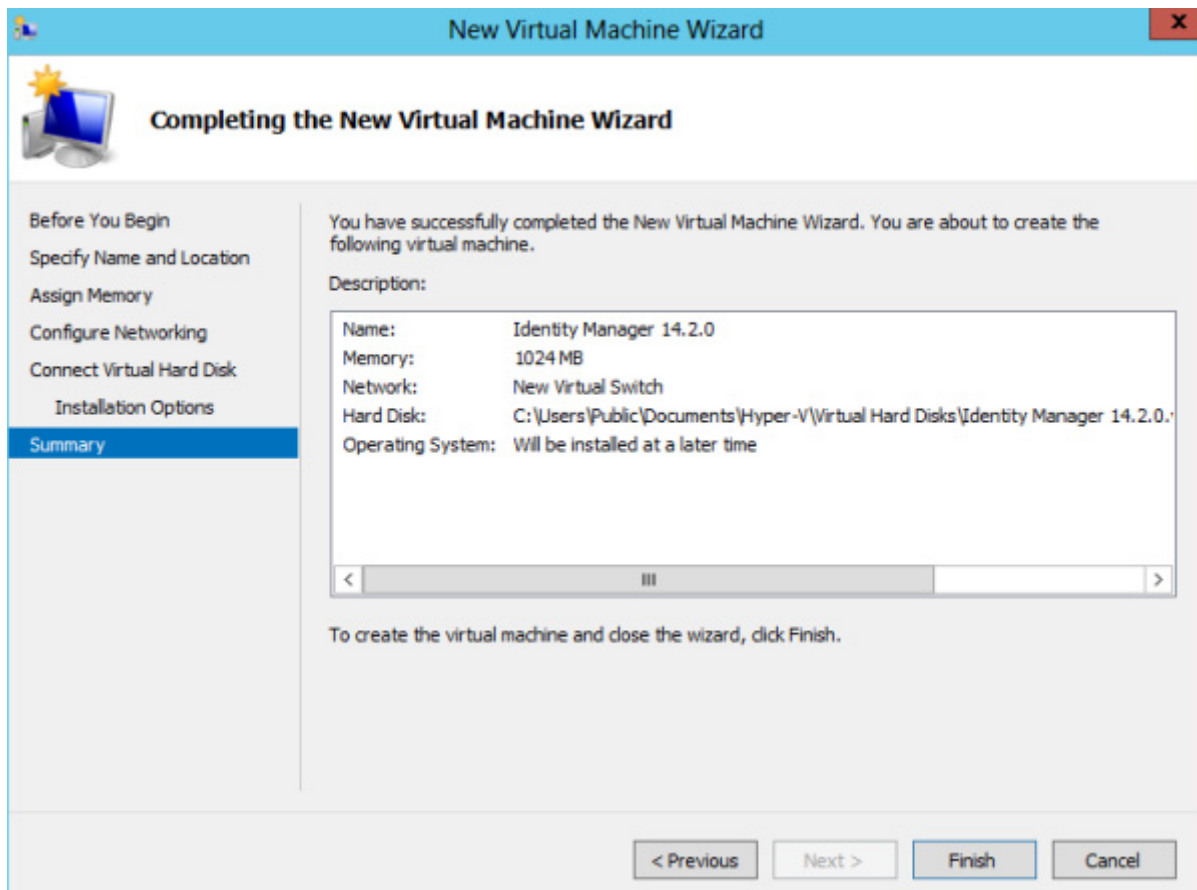
6. The Connection is set to your default switch, click on Next.



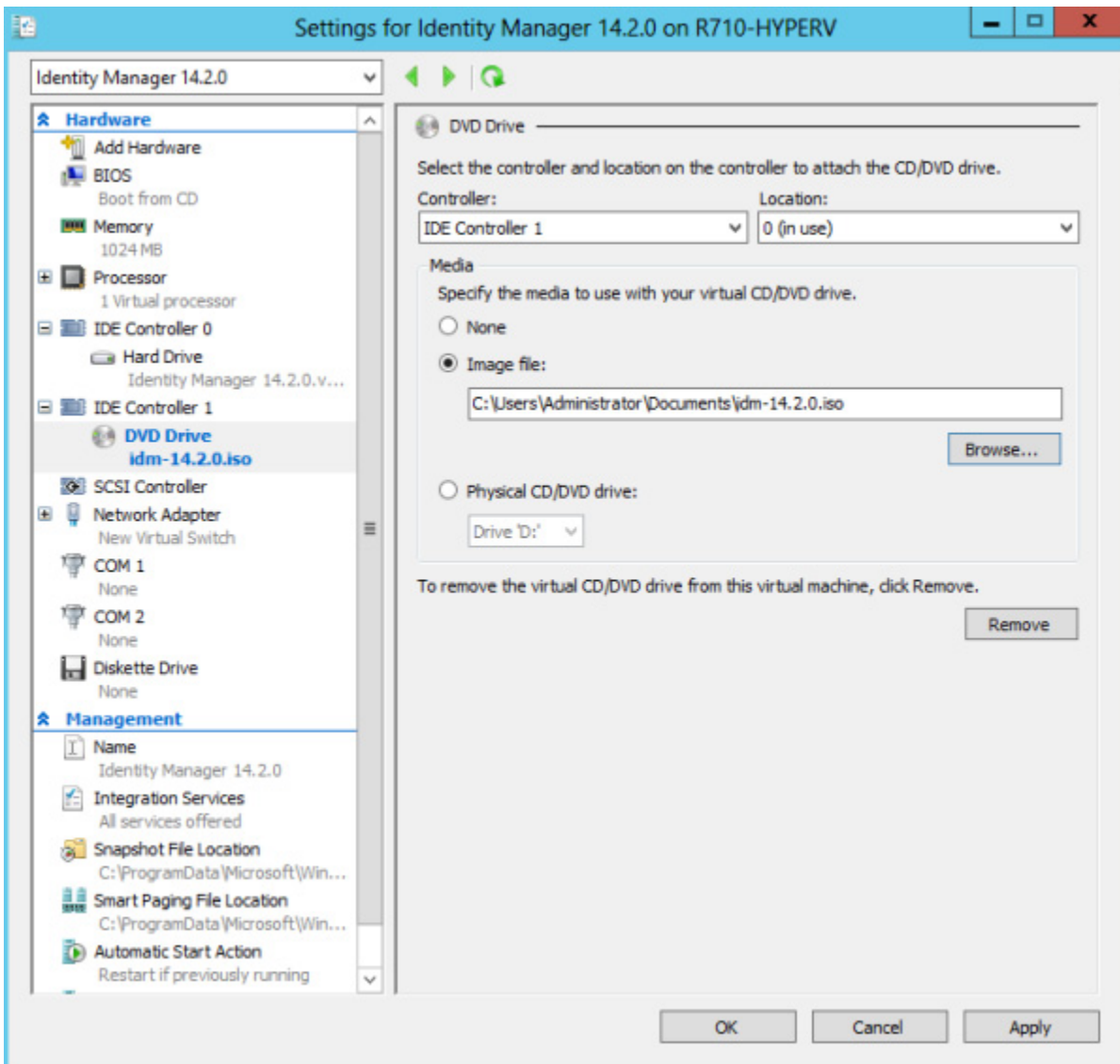
7. Choose a Disk size with a minimum of 50Gb (test and lab environments), minimum 100Gb for live environments (thin provisioning recommended where necessary), then click on Next to continue.



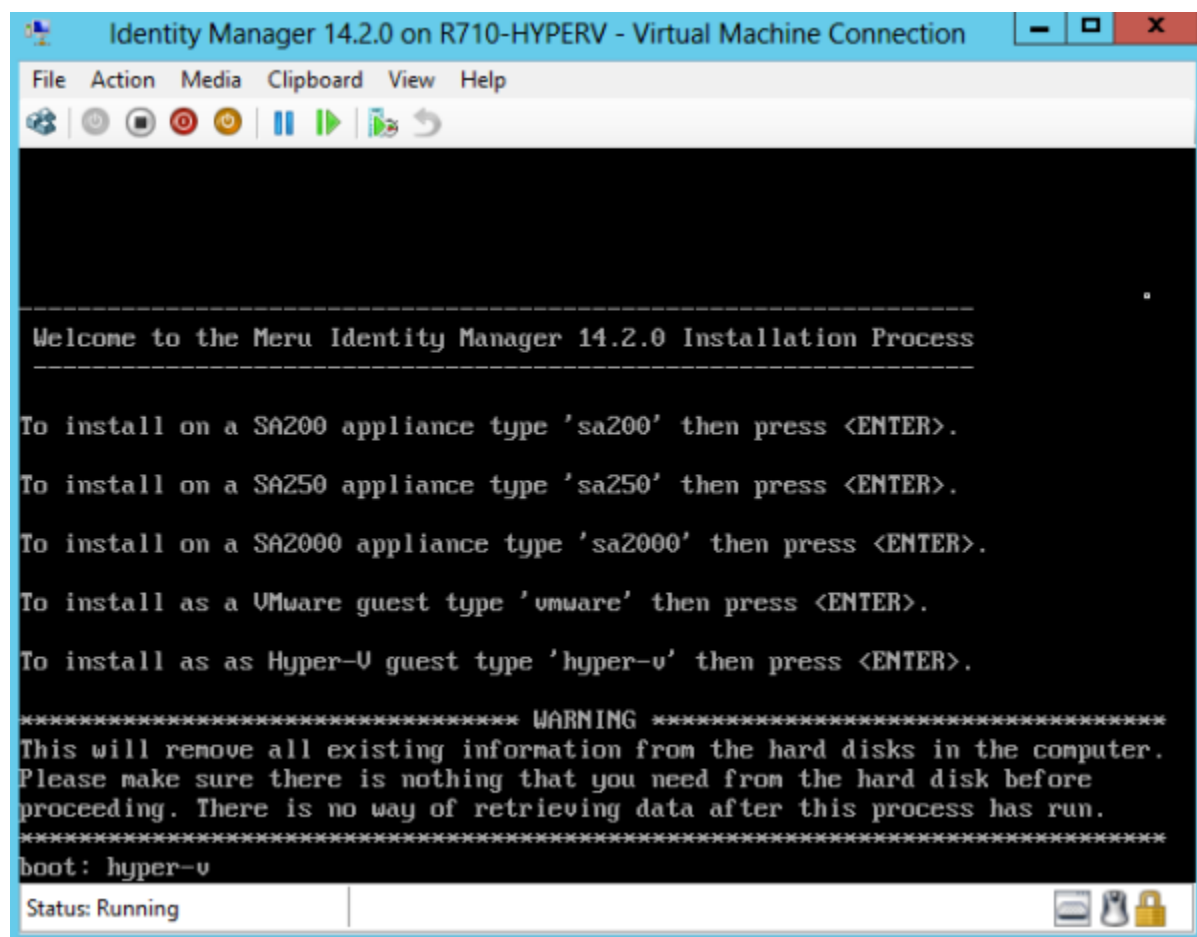
8. Ensure that the Install an operating system later option is checked then click on Next.



9. You have now finished creating your virtual machine, click on Finish to continue.
10. You will now see your virtual machine listed in Virtual Machines column, right click on your machine and click on the Settings option.
11. You will be presented with the settings screen as shown below.



12. To select and install your FortiConnect image file, click on the DVD Drive option underneath the IDE Controller 1 section in the Hardware column.
13. To the right of the screen, select the Image file check box and browse to the required iso image.
14. Right click on your virtual machine and click on the Start option.



15. Install FortiConnect by typing in hyper-v and hitting return.
16. The install can take around 5-10 minutes and may appear to pause at times. When the login prompt appears installation is complete.

Installing FortiConnect on SA200/SA250/SA2000

To install the FortiConnect onto a SA200/SA250 or SA2000 appliance you need to image the appliance to factory defaults, you can download the system image ISO from the support portal and burn this file to a blank CD-ROM.

- Burn an image with Windows 7 - To do this you can get the relevant info from <http://windows.microsoft.com/en-GB/windows/Burn-a-CD-or-DVD-from-an-ISO-file> . For other

versions of Windows, third-party disk burning tools may be required.

- Burn an image with Linux - For Linux right-click the image file and select *Write to disk*.

Once you have the system image on a bootable CD, you can perform the following steps to install the system image onto the SA200/SA250/SA2000.

1. Perform the installation over a serial console connection, attach a console management cable to the serial port on the back of the appliance. From the computer to which the serial cable is attached, run a terminal emulation program with settings set to: 115200 baud, 8 data bits, no parity, 1 stop bit, no flow control.
 - To connect using a Windows computer you will require a terminal application (e.g. PuTTY <http://www.chiark.greenend.org.uk/~sgtatham/putty/>)
 - To connect using a Linux computer you may use a GTKTerm. Depending on the distribution you use your user may have to be joined to the "dialout" group.
2. Once you have connected to the SA200/SA250/SA2000 appliance, insert the bootable CD into an external CD-ROM drive and attach it to the a one of the USB ports on the appliance.

Generic external USB CDROM drives can be used. The following drives have been tested and work correctly:

- Samsung External DVD Writer SE-S084
 - Lite On DVD ROM eTDU-108
 - Lenovo 43N3264 External USB DVD Writer
3. Power on the appliance. If the appliance is already started, switch it off and then switch it on again.
 4. The appliance should now boot from the CD-ROM drive and the initial install is displayed as shown below.

```
-----
Welcome to the Meru Connect 14.10.0 Installation Process
-----

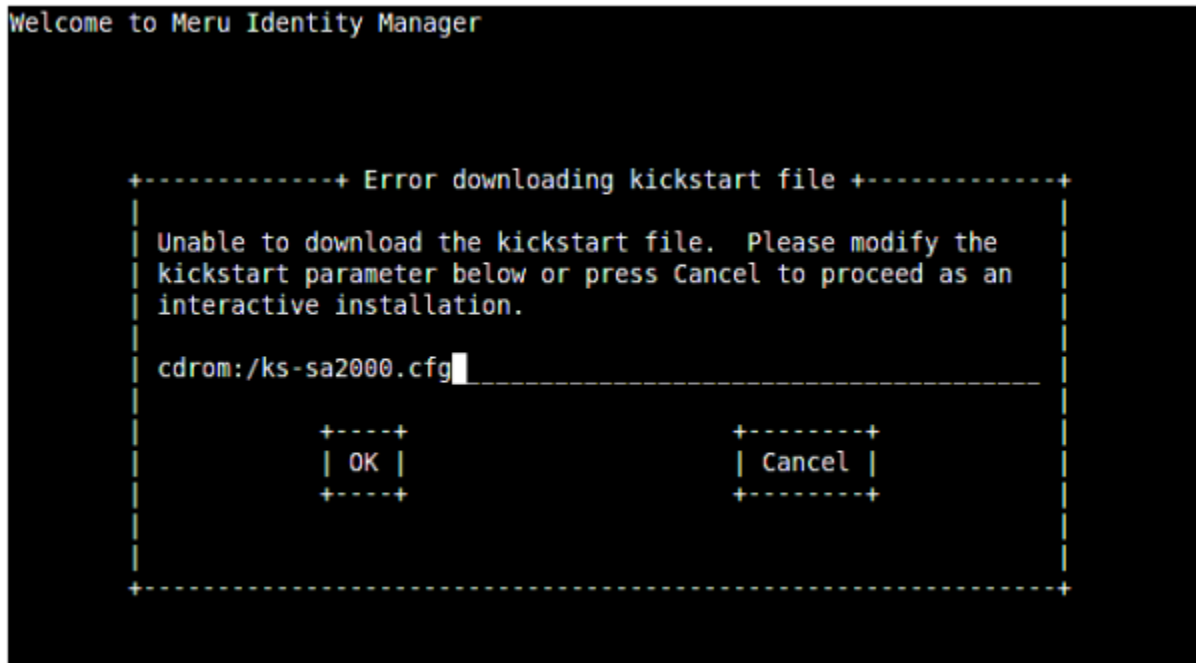
To install on a SA200 appliance type 'sa200' then press <ENTER>.
To install on a SA250 appliance type 'sa250' then press <ENTER>.
To install on a SA2000 appliance type 'sa2000' then press <ENTER>.
To install as a VMware guest type 'vmware' then press <ENTER>.
To install as a Hyper-V guest type 'hyper-v' then press <ENTER>.

***** WARNING *****
This will remove all existing information from the hard disks in the computer.
Please make sure there is nothing that you need from the hard disk before
proceeding. There is no way of retrieving data after this process has run.
*****
boot: _
```

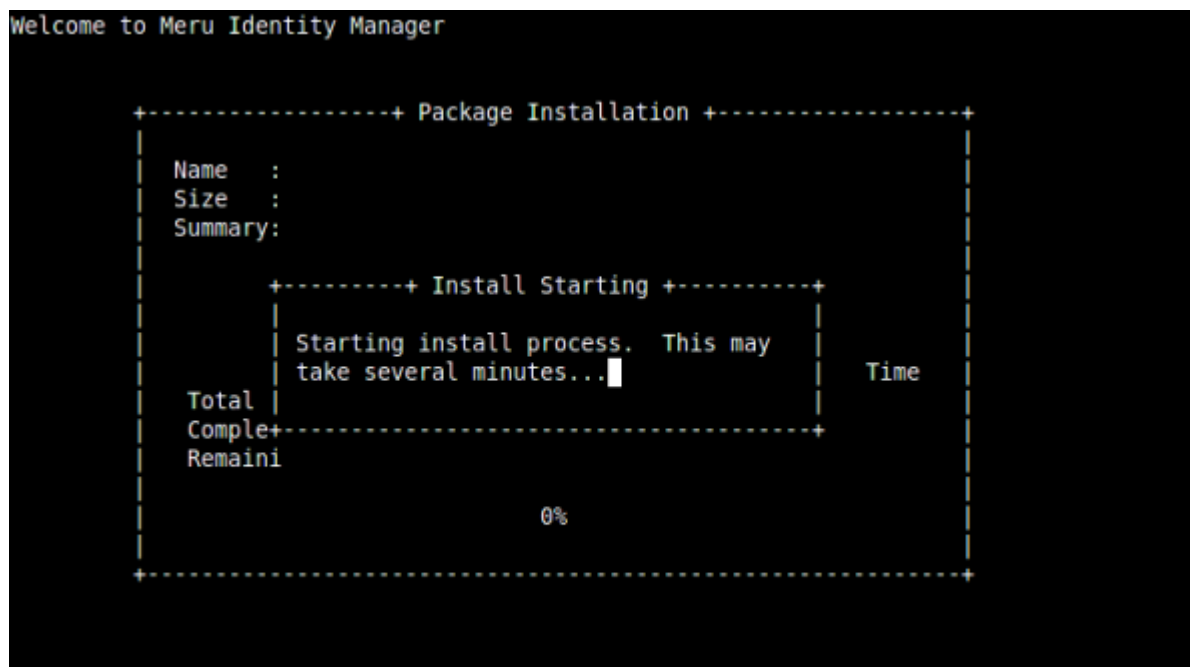
5. At the Initial Installation, run the installation according to the method you are connected to the appliance:

- If you are installing on a SA200 type *sa200* and press <Enter>.
- If you are installing on a SA250 type *sa250* and press <Enter>.
- If you are installing on a SA2000 type *sa2000* and press <Enter>.

Note: Some models of CDROM will 'go to sleep' too quickly after the menu is displayed. If this happens you will see the following confirmation dialog. Press <Enter> twice to continue installation.



6. The system image is automatically installed on the hard disk as shown below.



7. When the install image is successfully transferred, the system reboots automatically as shown below.

```
sending termination signals...done
sending kill signals...done
disabling swap...
/tmp/sda2
unmounting filesystems...
/mnt/runtime done
disabling /dev/loop0
/proc/bus/usb done
/proc done
/dev/pts done
/sys done
/tmp/ramfs done
/selinux done
/mnt/sysimage/boot done
/mnt/sysimage/sys done
/mnt/sysimage/proc/sys/fs/binfmt_misc done
/mnt/sysimage/proc done
/mnt/sysimage/selinux done
/mnt/sysimage/dev done
/mnt/sysimage done
rebooting system
```

8. The CD-ROM automatically ejects from the appliance.

Note: Some top-loading CDROM drives may not eject correctly following install. If this occurs, you will see an initial boot screen again as the CD is reread. It is safe to remove the CD manually and restart the server using the power switch.

9. The FortiConnect appliance boots and runs the final setup of the image automatically. The imaging process is complete when the login is displayed as shown below.

```
Meru Connect 14.10.0
localhost login: _
```

10. Continue to the instructions in the System Setup chapter to complete the installation.

System Setup

FortiConnect is administered using a web interface over either HTTP or HTTPS, or via the FortiConnect CLI. However, after initial installation, the system needs to be configured through the CLI to provide the networking configuration for the appliance so it can be accessed via the web interface to perform other admin tasks.

This chapter includes the following sections:

- Command Line Configuration
- Installing the Product License and Accessing the Administration Interface
- Setup Wizard
- Configuring Network Settings
- Date and Time Settings
- Configuring SSL Certificates
- Configuring Administrator Authentication

Command Line Configuration

To perform an initial configuration of the FortiConnect perform the following steps:

- Change the root password
- Configure IP Address and Default Gateway so that the appliance can be accessed on the network.

Initial Login

When logging in for the first time after initial installation, or after re-imaging the appliance, you need to set up a password for the root user.

1. Connect to the command line interface using either a keyboard and monitor connection to the appliance, or serial console connection.
2. Login as the root user. The login user name for the console is root as shown below.

```
Meru Connect 14.10.8  
localhost login: root  
You are required to change your password immediately (root enforced)  
New UNIX password: _
```

3. Change the password at the root prompt. Type a password and then confirm the password by re-entering it at the prompt. Once completed you will be presented with the CLI Administration Menu as shown below.

Note: Fortinet recommends using a strong password that is not based on a dictionary word, has a minimum of 6 characters, and contains at least 4 different characters.

```
Administration Menu  
-----  
1) About  
2) Network Settings  
3) Authentication  
4) Date & Time Settings  
5) Troubleshooting  
6) Certificates  
7) Upgrade  
8) Restore Backup  
9) Shutdown / Reboot  
X) Logout  
  
Option: _
```


About

From the CLI Administration Menu, you can check your system information by selecting menu option 1. This will bring up the screen below.

```
About
-----

Software: Meru Connect 14.10.0.0 Build 754

Platform: vmware

IP Address: 192.168.137.20

Hostname: localhost.localdomain

Serial Number: VMware-56 4d b3 0c ac 5e ee 10-9c d3 f8 4f a6 de 56 f5

System ID: ce74-4745-a4d3-8fa7-a693-30df-6e91-0ca2-7344-9166

Disk space: 35G total, 32G free

X) Exit to main menu

Option: _
```

From here we can see the following:-

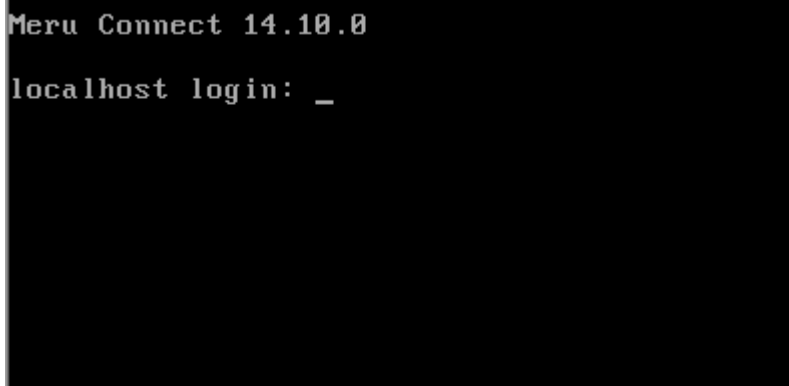
- Software - Version of FortiConnect
- Platform - Platform installed on.
- IP Address - IP Address of FortiConnect
- Hostname - Hostname
- Serial Number - Serial Number of FortiConnect
- System ID - System ID of FortiConnect
- Disk space - Total disk space and disk space free

Press X to exit out of the screen

Network Settings

To allow the appliance to be accessed on the network, you need to configure the IP address and default gateway for the first interface on the appliance (eth0 or NIC1). To configure these details, perform the following steps.

1. Using either a keyboard and monitor connection to the appliance, or serial console connection, authenticate to the command line interface as shown below. The username for the console is root and the password is the one you have previously configured.



```
Meru Connect 14.10.0
localhost login: _
```

2. You will be then presented with the CLI Administration Menu screen as show below, select menu option 2 to configure the Network Settings.

```
Administration Menu
-----
1) About
2) Network Settings
3) Authentication
4) Date & Time Settings
5) Troubleshooting
6) Certificates
7) Upgrade
8) Restore Backup
9) Shutdown / Reboot
X) Logout

Option: _
```

3. Choose from the numbered menu options which interface you would like to enter the network settings for, see below.

```
-----
1) Change eth0 IP Address [192.168.137.20]
2) Change eth0 Subnet Mask [255.255.255.0]
3) Change Default Gateway [192.168.137.2]
4) Change DNS Server 1 [192.168.137.2]
5) Change DNS Server 2 []
6) Enable IPv6 [disabled]
X) Exit to main menu

Option: _
```

- Select option number 1 to change the eth0 IP Address
- Select option number 2 to change the eth0 Subnet Mask
- Select option number 3 to change the Default Gateway
- Select option number 4 to change the DNS Server 1 Address
- Select option number 5 to change the DNS Server 2 Address (if a secondary DNS server is

configured on the network)

- Select option number 6 to enable IPv6 and change the settings (see step 6 on how to do this)
- To apply the changes press A
- Select X to Exit to the main menu

4. When an option has been selected, you can enter the new settings as shown below and then press Enter once complete.

```
Networks Settings
-----
1) Change eth0 IP Address [192.168.137.20]
2) Change eth0 Subnet Mask [255.255.255.0]
3) Change Default Gateway [192.168.137.2]
4) Change DNS Server 1 [192.168.137.2]
5) Change DNS Server 2 []
6) Enable IPv6 [disabled]
X) Exit to main menu

Option: 1
Enter new IP Address [192.168.137.20]: _
```

5. You will then be asked whether you wish to proceed with the changes, press A on your keyboard to proceed and a restart of your services will commence (press X on your keyboard to cancel this).
6. If you selected option number 6 to change IPv6 settings then you will be presented with the screen below and notice that IPv6 is now enabled.

```

Networks Settings
-----
* YOU MUST APPLY ETH0 CHANGES *

1) Change eth0 IP Address [192.168.137.20]
2) Change eth0 Subnet Mask [255.255.255.0]
3) Change Default Gateway [192.168.137.2]
4) Change DNS Server 1 [192.168.137.2]
5) Change DNS Server 2 []
6) Disable IPv6 [enabled]
7) IPv6 Address []
8) IPv6 Prefix Length [64]
9) IPv6 Gateway []

A) Apply eth0 Changes [IP Address / Subnet Mask / Default Gateway]
X) Exit to main menu

Option: _

```

- Select option 7 to enter the IPv6 Address
- Select option 8 to enter the IPv6 Prefix Length
- Select option 9 to enter the IPv6 Gateway

Once an option has been selected you can enter the details as shown on the screenshot above and press Enter

Alternatively, select option 6 to disable IPv6

Note: If you select one of the above options but do not wish to change any settings, hit Enter on your keyboard and you will return to the menu without any changes.

Authentication

Select the Authentication option to change root passwords on FortiConnect and change the Administration Admin password.

1. From the CLI Administration Menu select option 3 as shown below.

```
Administration Menu
-----

1) About
2) Network Settings
3) Authentication
4) Date & Time Settings
5) Troubleshooting
6) Certificates
7) Upgrade
8) Restore Backup
9) Shutdown / Reboot
X) Logout

Option: _
```

2. Select option 1 to change the root password on the appliance, enter the new password and then confirm.

```
Authentication
-----

1) Change Root Password
2) Reset Admin Interface Admin User Password
X) Exit to main menu

Option: 1
Are you sure? (y/n): y
New UNIX password: _
```

3. Select option 2 to Reset the Administration Interface Admin User Password, press Y to reset back to default settings.

```
Authentication
-----
1) Change Root Password
2) Reset Admin Interface Admin User Password
X) Exit to main menu

Option: 2
Are you sure? (y/n): _
```

Or press X to return to the main menu.

Date and Time Settings

Changing the Date and Time Settings on FortiConnect

1. To change the Date and Time Settings on FortiConnect select option 4 from the CLI Administration Menu

```
Administration Menu
-----

1) About
2) Network Settings
3) Authentication
4) Date & Time Settings
5) Troubleshooting
6) Certificates
7) Upgrade
8) Restore Backup
9) Shutdown / Reboot
X) Logout

Option: _
```

2. From the menu options shown below, you can change the Date and Time Settings

```
Date & Time Settings
-----

Current local time 2013-06-10 06:28:15

1) Set Timezone [America/Los_Angeles]
2) Set Time [06:28:15]
3) Set Date [2013-06-10]
X) Exit to main menu

Option: _
```

3. Select menu option 1 to set the timezone for FortiConnect.


```
Select Timezone [page 1 / 17]
-----
01) Africa/Abidjan          02) Africa/Accra
03) Africa/Addis_Ababa     04) Africa/Algiers
05) Africa/Asmara          06) Africa/Asmera
07) Africa/Bamako          08) Africa/Bangui
09) Africa/Banjul          10) Africa/Bissau
11) Africa/Blantyre        12) Africa/Brazzaville
13) Africa/Bujumbura       14) Africa/Cairo
15) Africa/Casablanca      16) Africa/Ceuta
17) Africa/Conakry         18) Africa/Dakar
19) Africa/Dar_es_Salaam   20) Africa/Djibouti
21) Africa/Douala          22) Africa/El_Aaiun
23) Africa/Freetown        24) Africa/Gaborone
25) Africa/Harare          26) Africa/Johannesburg
27) Africa/Kampala         28) Africa/Khartoum
29) Africa/Kigali          30) Africa/Kinshasa
31) Africa/Lagos           32) Africa/Libreville
33) Africa/Lome            34) Africa/Luanda

X) Exit selection          N) Next Page

Option [type choice & press enter]:
```

- Select your geographical location using the numbers provided and press Enter. Navigate through the Continents and Cities by clicking on N to see the next page.

Services will now restart on your machine so the settings can be implemented.

4. Select menu option 2 to set the Time of the FortiConnect.

```
Date & Time Settings
-----

Current local time 2013-06-10 06:29:49

1) Set Timezone [America/Los_Angeles]
2) Set Time [06:29:49]
3) Set Date [2013-06-10]
X) Exit to main menu

Option: 2
Enter new time (hh:mm:ss) [06:29:49]: _
```

- Enter your required time and press Enter, the time will set automatically.

5. Select menu option 3 to set the Date for FortiConnect.

```
Date & Time Settings
-----

Current local time 2013-06-10 06:31:20

1) Set Timezone [America/Los_Angeles]
2) Set Time [06:31:20]
3) Set Date [2013-06-10]
X) Exit to main menu

Option: 3
Enter new date (yyyy-mm-dd) [2013-06-10]: _
```

- Enter the Date you require and press Enter and the date will set automatically.

Select X to return to the main menu.

Trouble Shooting

The CLI Administration Menu allows you access to a Troubleshooting menu.

1. From the CLI Administration Menu as shown below select option 5.

```
Administration Menu
-----

1) About
2) Network Settings
3) Authentication
4) Date & Time Settings
5) Troubleshooting
6) Certificates
7) Upgrade
8) Restore Backup
9) Shutdown / Reboot
X) Logout

Option: _
```

This will bring up the CLI Troubleshooting menu as shown below.

```
Troubleshooting
-----

1) Ping, DNS Lookup and Traceroute
2) Show Routing Table
3) Show System Processes [Type q to exit]
4) Show Service Status
5) Enter Engineering Mode
6) Clear Allowed IP Addresses
7) Show Critical Alerts
8) Clear Root Password and Power Off
9) Extend Disk Space
X) Exit to main menu

Option: _
```

2. From the CLI Troubleshooting menu, select option 1 to open the Ping, DNS Lookup and Traceroute menu.

```
Ping, DNS Lookup and Traceroute
```

- ```

1) Ping
2) DNS Lookup
3) Traceroute
X) Exit to previous menu
```

```
Option: _
```

3. To ping a device select option 1 Ping.

```
Ping, DNS Lookup and Traceroute
```

- ```
-----  
1) Ping  
2) DNS Lookup  
3) Traceroute  
X) Exit to previous menu
```

```
Option: 1  
IPv4 Address / IPv6 Address / Domain Name to Ping: _
```

4. Enter either the IPv4, IPv6 or the Domain Name of the device to ping and press Enter. Your ping results will appear.
5. To perform a DNS Lookup select option 2 DNS Lookup.

Ping, DNS Lookup and Traceroute

- 1) Ping
- 2) DNS Lookup
- 3) Traceroute
- X) Exit to previous menu

Option: 2

IPv4 Address / IPv6 Address / Domain Name to lookup in DNS: _

6. Enter either the IPv4, IPv6 or the Domain Name to lookup in DNS and press Enter. Your DNS Lookup results will appear.
7. To perform a Traceroute select option 3 Traceroute

Ping, DNS Lookup and Traceroute

- 1) Ping
- 2) DNS Lookup
- 3) Traceroute
- X) Exit to previous menu

Option: 3

IPv4 Address / IPv6 Address / Domain Name to Traceroute: _

8. Once complete press X to return to the previous menu.
9. From the CLI Troubleshooting menu, select option 2 to Show a Routing Table. Press enter to return to the Troubleshooting menu.

```

Routing Table
-----

IP Routing Table
Destination      Gateway           Netmask           Flags    MSS Window  irtt Iface
192.168.137.0    *                 255.255.255.0    U        0 0      0 eth0
169.254.0.0      *                 255.255.0.0      U        0 0      0 eth0
default          192.168.137.2    0.0.0.0          UG       0 0      0 eth0

X) Return to previous menu

Option: _

```

10. From the CLI Troubleshooting menu, select option 3 to Show System Processes. Press q to quit from this screen and then press X to return to the Troubleshooting menu.

```

top - 07:26:25 up 42 min,  1 user,  load average: 0.92, 0.77, 0.51
Tasks:  95 total,   1 running,  94 sleeping,   0 stopped,   0 zombie
Cpu(s):  0.3%us,  1.0%sy,  0.0%ni, 98.0%id,  0.3%wa,  0.0%hi,  0.3%si,  0.0%st
Mem:   1834720k total,   316044k used,   718676k free,   18012k buffers
Swap:  2048276k total,    0k used,   2048276k free,   186340k cached

  PID USER      PR  NI  VIRT  RES  SHR  S  %CPU  %MEM    TIME+  COMMAND
 6924 root        18   0 37976 20m 6884 S   0.7   2.0   0:00.31 php
    1 root        15   0  2160   668  576 S   0.0   0.1   0:01.28 init
    2 root         RT  -5     0     0     0 S   0.0   0.0   0:00.00 migration/0
    3 root        34  19     0     0     0 S   0.0   0.0   0:00.00 ksoftirqd/0
    4 root        10  -5     0     0     0 S   0.0   0.0   0:00.00 events/0
    5 root        18  -5     0     0     0 S   0.0   0.0   0:00.00 khelper
    6 root        19  -5     0     0     0 S   0.0   0.0   0:00.00 kthread
    9 root        10  -5     0     0     0 S   0.0   0.0   0:00.03 kblockd/0
   10 root        20  -5     0     0     0 S   0.0   0.0   0:00.00 kacpid
  174 root        14  -5     0     0     0 S   0.0   0.0   0:00.00 cqueue/0
  177 root        10  -5     0     0     0 S   0.0   0.0   0:00.00 khubd
  179 root        10  -5     0     0     0 S   0.0   0.0   0:00.00 kseriod
  242 root        15   0     0     0     0 S   0.0   0.0   0:00.00 khungtaskd
  243 root        16   0     0     0     0 S   0.0   0.0   0:00.00 pdflush
  244 root        15   0     0     0     0 S   0.0   0.0   0:00.85 pdflush
  245 root        11  -5     0     0     0 S   0.0   0.0   0:00.00 kswapd0
  246 root        11  -5     0     0     0 S   0.0   0.0   0:00.00 aio/0
  465 root        19  -5     0     0     0 S   0.0   0.0   0:00.00 kpsmoused

```

11. From the CLI Troubleshooting menu, select option 4 to Show Service Status. Press X to return to the Troubleshooting menu.

```

Service Status
-----

crond started
httpd started
ldap stopped
logprocd started
manualcrld started
memcached started
network started
ntpd stopped
postgresql started
radiusd started
twin stopped

X) Return to previous menu

Option: _

```

12. From the CLI Troubleshooting menu, select option 5 to Enter Engineering Mode. Engineering mode is provided so that technical support can help perform any low level debugging that is needed.

```

Troubleshooting
-----

1) Ping, DNS Lookup and Traceroute
2) Show Routing Table
3) Show System Processes [Type q to exit]
4) Show Service Status
5) Enter Engineering Mode
6) Clear Allowed IP Addresses
7) Show Critical Alerts
8) Clear Root Password and Power Off
9) Extend Disk Space
X) Exit to main menu

Option: 5

Engineering Client Code: e178-ah0q-65a4
Enter Engineering Response Code: _

```

13. From the CLI trouble shooting menu, select option 6 to Clear Allowed IP Addresses. Select *y* to continue or *n* to cancel.

```
Troubleshooting
-----

1) Ping, DNS Lookup and Traceroute
2) Show Routing Table
3) Show System Processes [Type q to exit]
4) Show Service Status
5) Enter Engineering Mode
6) Clear Allowed IP Addresses
7) Show Critical Alerts
8) Clear Root Password and Power Off
9) Extend Disk Space
X) Exit to main menu

Option: 6
Are you sure? (y/n): _
```

14. From the CLI trouble shooting menu, select option 7 to Show Critical Alerts. A list of critical alerts should be displayed. If there are no critical alerts you should see the screen as shown below.

```
Troubleshooting
-----

* NO ALERTS TO DISPLAY *

1) Ping, DNS Lookup and Traceroute
2) Show Routing Table
3) Show System Processes [Type q to exit]
4) Show Service Status
5) Enter Engineering Mode
6) Clear Allowed IP Addresses
7) Show Critical Alerts
8) Clear Root Password and Power Off
9) Extend Disk Space
X) Exit to main menu

Option: _
```

Note: Option 8 - Clear Root Password and Power Off is for Fortinet internal use only and should not be used.

15. From the CLI trouble shooting menu, select option 9 to Extend Disk Space on your virtual machine.

```
New disk found with 80G of space

Your current free space is 777G

Your total free space would increase to 857G

As this process modifies your disks configuration we require that the following
steps are taken before continuing:

1. Take a backup, and ensure this is stored on an external system
2. Take a Hyper-V snapshot

The process will take some time, during which the system will not be available
for use.

Do you wish to continue? (y/n): y
```

Note: Add an additional physical disk in the server if the physical disk space is insufficient and then select 9 to extend disk space in your virtual machine.

16. If disk space is found you will be then advised to take the relevant snapshots before continuing. Type N to exit and take a snapshot, or Y to continue.

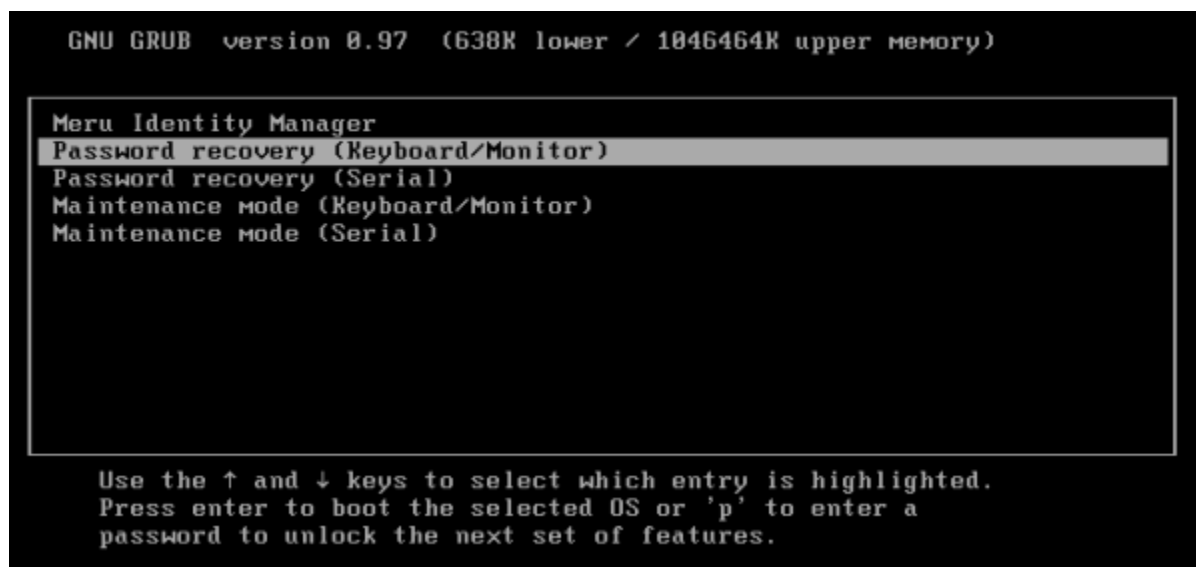
Root Password Reset

In the rare occurrence you may need to reset your Root Password you will have to manually reboot FortiConnect first.

1. Once you have rebooted press any key when you see the screen below.

```
GRUB Loading stage2...  
Press any key to continue.  
Press any key to continue.  
Press any key to continue.  
_
```

You will then see the screen as shown below.



2. Use the arrow keys on your keyboard to highlight Password Recovery (Keyboard/Monitor) if using a keyboard and monitor to connect, or highlight Password Recovery (Serial) if attached to an appliance (SA200/SA250/2000)
3. Press Enter
4. Enter your new root password by following the instructions on the screen below.

```
Password Recovery Mode
-----
Changing password for user root.
New UNIX password:
Retype new UNIX password: _
```

5. Enter your new password and press enter.
6. Retype your new password and press enter.

You have now successfully changed your root password and will be returned to the root login prompt.

Certificates

Server Certificate administration can be managed within the CLI Administration Menu.

1. From the CLI Administration Administration Menu, select menu option 6.

```
Administration Menu
-----

1) About
2) Network Settings
3) Authentication
4) Date & Time Settings
5) Troubleshooting
6) Certificates
7) Upgrade
8) Restore Backup
9) Shutdown / Reboot
X) Logout

Option: _
```

2. To create a temporary certificate select option 1.

```
Certificates
-----

1) Create Temporary Certificate
2) Regenerate Private Key & Create Temporary Certificate
X) Exit to main menu

Option: _
```

- The certificate will be automatically created and FortiConnect will reboot and return you to the root login after. Further information on certificates and FortiConnect are explained later in the documentation.

3. To Regenerate a Private Key and Create a Temporary Certificate select option 2.

```
Certificates
-----
1) Create Temporary Certificate
2) Regenerate Private Key & Create Temporary Certificate
X) Exit to main menu

Option: _
```

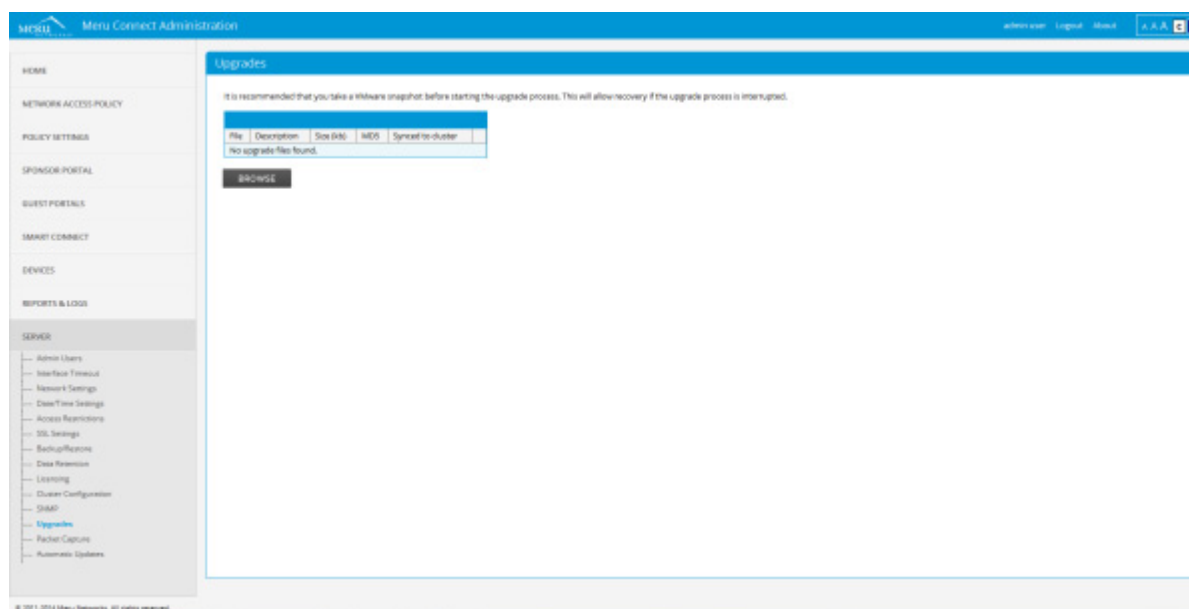
- The Private Key will be regenerated and the certificate will be automatically created and the FortiConnect will reboot and return you to the root login after. Further information on certificates and the FortiConnect are explained later in the documentation.

Upgrade

From the CLI Administration menu you can perform an upgrade of FortiConnect. To allow this you must have already uploaded the upgrade file to your FortiConnect appliance, this can be done via the FortiConnect administration interface once you have logged on for the first time (Please see section System Setup on how to log on and use FortiConnect Administration).

1. From the FortiConnect Administration Interface select Server and click on Upgrades as shown below.

Upgrade



2. Click on the browse button and select the upgrade file from your locally stored directory. The file should upload automatically.
3. From the CLI Administration Menu select option 7.

Note: PLEASE NOTE THAT FORTICONNECT 14.10 CAN ONLY BE UPGRADED FROM Identity Manager RELEASES 13.10 and 14.2

Note: The FortiConnect upgrade should be run when connected to the FortiConnect console, if you run the upgrade via SSH please ensure network connectivity is maintained throughout the duration of the upgrade, loss of connectivity may cause the upgrade to fail.

Note: IMPORTANT - DEPENDING ON THE AMOUNT OF DATA IN THE FORTICONNECT DATABASE THIS UPGRADE PROCESS MAY TAKE A SHORT WHILE, PLEASE DO NOT ABORT THE PROCESS EVEN IF IT DOESNT LOOK APPARENT THAT PROCESSES ARENT RUNNING

```
Administration Menu
-----

1) About
2) Network Settings
3) Authentication
4) Date & Time Settings
5) Troubleshooting
6) Certificates
7) Upgrade
8) Restore Backup
9) Shutdown / Reboot
X) Logout

Option: _
```

4. The file you uploaded in step 2 should now be displayed next to option 1 in the CLI Upgrade menu. Select option 1 to perform the upgrade.

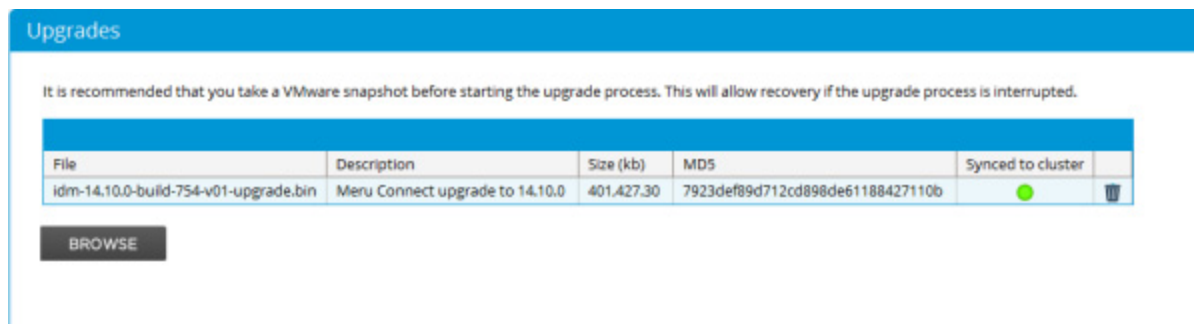
```
Upgrade
-----

1) Run upgrade_11.12.0.bin [Identity Manager upgrade to 11.12.0]
X) Exit to main menu

Option: _
```

5. If performing an upgrade across a cluster of FortiConnect appliances you will be able to push the upgrade across clusters, to do this go to Server --> Upgrades in the FortiConnect administration interface as shown below.
6. Click on the Push to cluster button to sync between clusters.

7. Once synced you will see the icon change to green as shown below.



Restore Backup

From the CLI Administration Interface you can Restore a Backup.

1. From the CLI Administration Menu select option 8.

```
Administration Menu
-----
1) About
2) Network Settings
3) Authentication
4) Date & Time Settings
5) Troubleshooting
6) Certificates
7) Upgrade
8) Restore Backup
9) Shutdown / Reboot
X) Logout

Option: _
```


2. Select which backup you wish to restore and press enter.

```
Restore Backup
-----
1) Restore guestbackup_13.2.0_20130205-170513.zip [2013-02-05 17:05]
X) Exit to main menu

Option: _
```

3. Press X to return to the main menu.

Shut Down / Reboot

From the CLI Administration Menu you can perform Shut Down and Reboot options of FortiConnect.

1. From the CLI Administration Menu select option 9.

```
Administration Menu
-----
1) About
2) Network Settings
3) Authentication
4) Date & Time Settings
5) Troubleshooting
6) Certificates
7) Upgrade
8) Restore Backup
9) Shutdown / Reboot
X) Logout

Option: _
```

2. Select menu option 1 to Shutdown FortiConnect, or menu option 2 to Reboot FortiConnect.

```
Shutdown / Reboot
-----
1) Shutdown server
2) Reboot server
X) Exit to main menu

Option: _
```

Logout

Logout of the CLI Administration Menu at any time by choosing X on the menu as shown below.

```
Administration Menu
-----
1) About
2) Network Settings
3) Authentication
4) Date & Time Settings
5) Troubleshooting
6) Certificates
7) Upgrade
8) Restore Backup
9) Shutdown / Reboot
X) Logout

Option: _
```

Installing the Product License and Accessing the Administration Interface

Before accessing the web administration interface of FortiConnect, you need to install a product license.

This section describes the following:

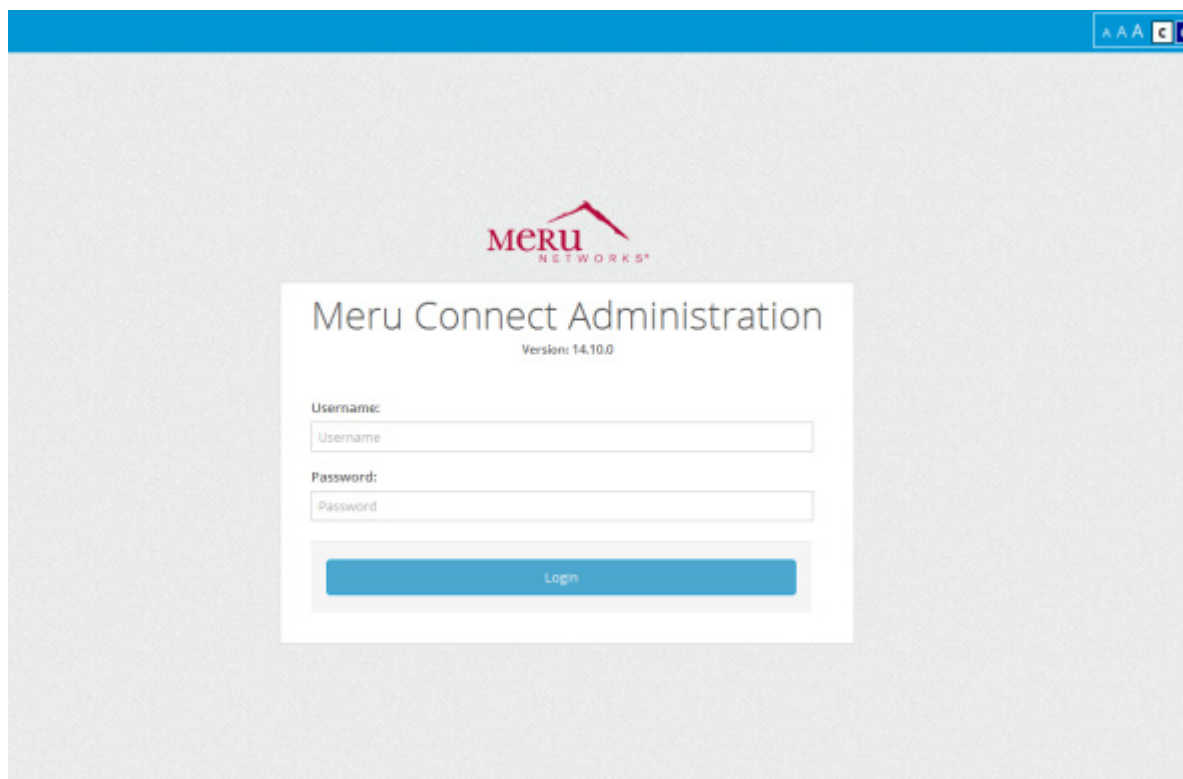
- Obtain and Install a FortiConnect License
- Access the FortiConnect Interface.

Obtain and Install a FortiConnect License

To obtain a product license please follow the instructions on the Entitlement Certificate that ships with the product.

Access the FortiConnect Interface

1. If you have installed a license, the admin login is automatically displayed. Otherwise, open a web browser to the FortiConnect Administration interface by entering the IP address that you configured through the command line as the URL, followed by /admin :
 - For HTTP access, open `http://<Forticonnect_ip_address>/admin`
 - For HTTPS access, open `https://<Forticonnect_ip_address>/admin`
2. The FortiConnect Administration interface is displayed as shown below. This is the administrator interface to the appliance.
3. Login as the admin user. The default user name/password for the admin console is admin/admin.



Note: Fortinet recommends setting up SSL access and also to change the default admin user password for security.

Note: Entering the FortiConnect Appliance IP address without the” /admin” as the URL brings up the Sponsor Interface, details about the Sponsor Interface are detailed later in the document.

Setup Wizard

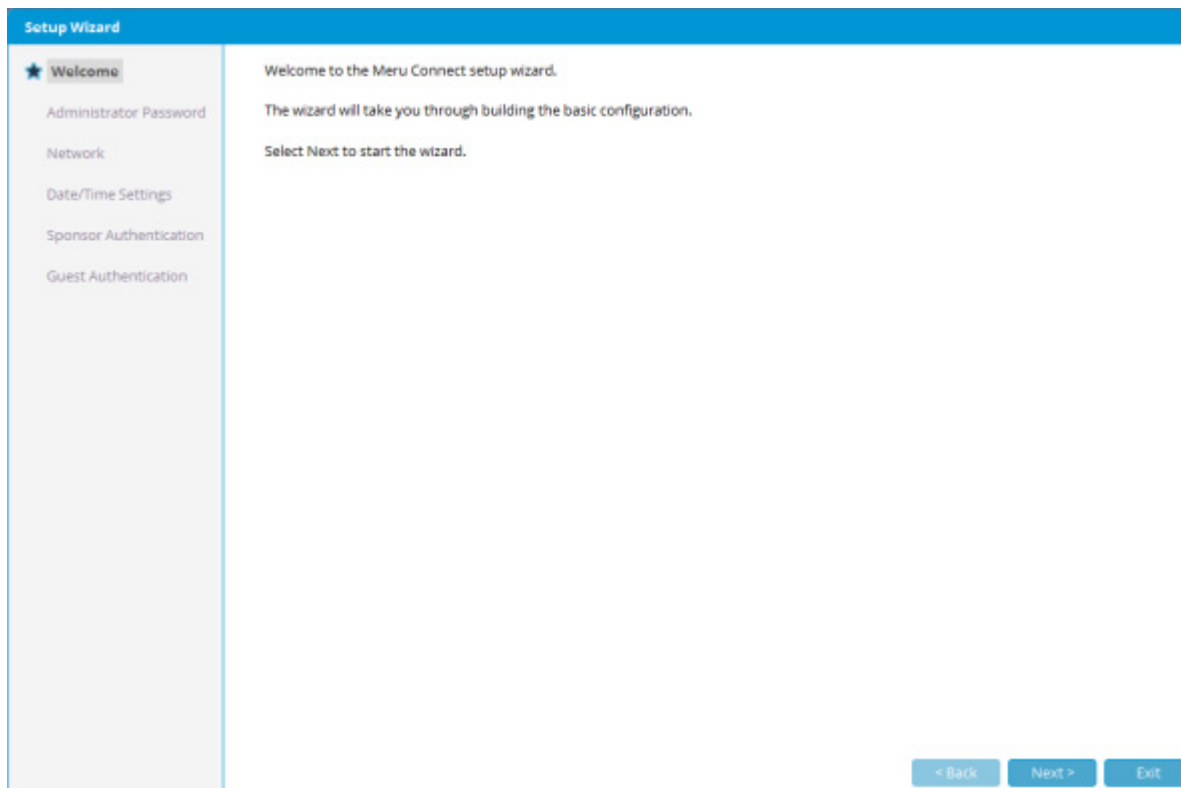
Getting started within FortiConnect is made easy using a Setup Wizard to help configure basic settings before performing any other operations. This minimizes the need to restart the appliance later on.

1. Upon logging into the FortiConnect Administration Interface for the first time the SetupWizard will automatically start as seen below.

Note: To access the Setup Wizard at anytime after exiting navigate to Home-->Setup Wizard

2. Click Next to continue.

Setup Wizard



Note: Clicking on the Exit button at anytime will exit the Setup Wizard and any changes made up to that point will be saved.

3. The next step in the Setup Wizard allows you to change the Administrator Password, this must be changed the first time you go through the setup wizard, the Administrator Password is the password for the default admin account. Enter and repeat the new password, or simply leave blank if you wish to keep the existing password.

Note: The password must be at least six characters and must contain at least four different characters

4. Click Next to continue

The screenshot shows the 'Setup Wizard' interface. On the left is a sidebar with a list of steps: 'Welcome' (checked), 'Administrator Password' (selected with a star), 'Network', 'Date/Time Settings', 'Sponsor Authentication', and 'Guest Authentication'. The main area displays a message: 'In order to continue the default admin password must be changed now.' Below this are two input fields labeled 'Admin Password:' and 'Confirm:'. A note below the fields states: 'Your password must be at least six characters long and contain a minimum of four different characters'. At the bottom right are three buttons: '< Back', 'Next >', and 'Exit'.

5. Now enter any DNS settings in the next step below, you will be required to enter :

- Hostname - Hostname of your server
- Domain - Domain name
- Primary DNS - IP address of Primary DNS server
- Secondary DNS - IP address of secondary DNS server

Note: If you don't setup a valid DNS server the setup process may take longer as DNS requests time out.

Setup Wizard

The screenshot shows the 'Setup Wizard' window with a blue header. On the left is a sidebar with a list of steps: 'Welcome' (checked), 'Administrator Password' (checked), 'Network' (selected with a star icon), 'Date/Time Settings', 'Sponsor Authentication', and 'Guest Authentication'. The main area is for network configuration. It contains four input fields: 'Hostname' with 'localhost' and '.localdomain' as a suffix, 'Domain' with 'localdomain', 'Primary DNS' with '192.168.137.2', and 'Secondary DNS' which is empty. At the bottom right are three buttons: '< Back', 'Next >', and 'Exit'.

Field	Value
Hostname	localhost.localdomain
Domain	localdomain
Primary DNS	192.168.137.2
Secondary DNS	

6. Click Next to continue
 7. You will then be required to enter in your Date/Time Settings as shown below, you can manually enter your Date/Time Settings or use an NTP server.
- Note:** Upon changing the date and time settings you will be shown a pop up message saying "Please wait, system services are being restarted". The system is rebooting to allow the date and time settings to take effect.

Setup Wizard

- ✓ Welcome
- ✓ Administrator Password
- ✓ Network
- ★ **Date/Time Settings**
- Sponsor Authentication
- Guest Authentication

NTP is used to automatically synchronize your server time. If your organization has its own NTP server(s) you should use them, if not you may be able to use servers from <http://www.pool.ntp.org>.

The system timezone is used by the server administrators (it affects shell logins, system services and the dates displayed in log files).

Date/Time

System Date: 1 Dec 2014

05:35:24

System Timezone: America/Los_Angeles

NTP

Use NTP to sync System Date & Time: ☐

NTP Server 1: 0.merunetworks.pool.ntp.org

NTP Server 2: 1.merunetworks.pool.ntp.org

NTP Server 3: 2.merunetworks.pool.ntp.org

< Back Next > Exit

NOTE: NTP is automatically used to synchronize server time. If your organization has your own NTP Server (s) use them, if not you may be able to use server (s) from <http://www.pool.ntp.org>.

- To Manually enter your Date/Time Settings - set the System Date using the Date Picker and System Timezone from the drop down menu.
- To use an NTP Server - Click inside the check box Use NTP to sync System Date & Time: and enter NTP server settings.

8. Click Next to continue

9. Then you can set up the Sponsor Authentication, below. Sponsors are users within your organization who are responsible for offering access to guests. Sponsor Authentication settings determine how these Sponsors are authenticated in FortiConnect.

Setup Wizard

The screenshot shows the 'Setup Wizard' window. On the left is a sidebar with a list of steps: 'Welcome', 'Administrator Password', 'Network', 'Date/Time Settings', 'Sponsor Authentication' (which is highlighted with a star and a blue background), and 'Guest Authentication'. The main area of the window contains text explaining that sponsors are users within the organization responsible for offering access to guests, and that settings determine how they are authenticated. It also mentions that additional authentication methods can be specified in the Sponsor Portal. Below this text, there is a form with two fields: 'Authentication Type' with a dropdown menu currently set to 'Microsoft Active Directory', and 'Server:' with a text input field. A small label 'Hostname or IP Address' is positioned below the 'Server:' input field. At the bottom right of the window are three buttons: '< Back', 'Next >', and 'Exit'.

10. From the Authentication Type dropdown menu, select from the following methods of Authentication (for the purpose of documentation the most popular methods have been captured below) :

Microsoft Active Directory - Enter Hostname or IP Address. Upon entering this, click Next and you will then be asked to enter more information

- Name - Server name
- Server - Server IP Address
- Domain - Server Domain Name
- Encryption - From the dropdown menu select the required encryption method.
- Base DN - Base DN information

With this information entered, click Next. You will then be prompted to enter the Search Credentials for the Active Directory server. Enter the appropriate Username and Password for your Active Directory server.

OpenLDAP - Enter Hostname or IP Address. Upon entering this, click Next and you will then be asked to enter more information

- Name - Server name
- Server - Server IP Address

- Encryption - From the dropdown menu select the required encryption method.
- Base DN - Base DN information

Novell eDirectory - Enter Hostname or IP Address

- Name - Server name
- Server - Server IP Address
- Encryption - From the dropdown menu select the required encryption method.
- Base DN - Base DN information

LDAP - Enter Hostname or IP Address

- Name - Server name
- Server - Server IP Address
- Encryption - From the dropdown menu select the required encryption method.
- Base DN - Base DN information

RADIUS - Enter Hostname or IP Address

- Name - Server name
- Server - Server IP Address
- Port - Port number
- Secret - Secret information, and confirm.

Internal Sponsor Database

- First name - First name of Sponsor to be created.
- Last name - Last name of Sponsor to be created.
- Email - Email Address of Sponsor to be created.
- User Name - User Name of Sponsor to be created.
- Password - Password and confirmation.
- Click Add to Add Sponsor

11. Click Next to continue

Note: If Sponsor Authentication has already been set up, you will see the screen below.

Setup Wizard

The screenshot shows the 'Setup Wizard' interface with a blue header. On the left is a sidebar with a list of steps: 'Welcome', 'Administrator Password', 'Network', 'Date/Time Settings', 'Sponsor Authentication' (highlighted with a star), and 'Guest Authentication'. The main area is titled 'Create local sponsors who are permitted to issue guest accounts.' It features a table with columns 'Username', 'First Name', 'Surname', 'Email', and 'Group'. Below the table is a button labeled 'Add'. To the right of the table are input fields for 'First Name', 'Last Name', 'Email', 'Username', 'Password', and 'Confirm'. At the bottom right are three buttons: '< Back', 'Next >', and 'Exit'.

Setup Wizard

- ✓ Welcome
- ✓ Administrator Password
- ✓ Network
- ✓ Date/Time Settings
- ★ **Sponsor Authentication**
- Guest Authentication

Create local sponsors who are permitted to issue guest accounts.

Username	First Name	Surname	Email	Group
No sponsors defined				

First Name:

Last Name:

Email:

Username:

Password: Confirm:

< Back Next > Exit

12. Then you can setup User Authentication as per below, Users are authenticated by network devices acting as a policy enforcement point in the network. These are normally the devices that intercept the Users web requests and redirect them to a login page.

Setup Wizard

- ✓ Welcome
- ✓ Administrator Password
- ✓ Network
- ✓ Date/Time Settings
- ✓ Sponsor Authentication
- ★ **Guest Authentication**

Guests are authenticated by network devices acting as the policy enforcement point in the network. These are normally the devices that intercept the guests web requests and redirect them to a login page.

Meru Connect supports authenticating the guests from these devices using RADIUS in the case of wireless controllers, LAN switches, firewalls etc.

Enter the details of the initial device that you would like to authenticate the guests.

Network Device Type: RADIUS

Network Device:

Hostname or IP Address

< Back
Next >
Exit

13. From the Network Device Type drop down menu, select which Authentication method you wish to use:

RADIUS - Enter the network device's IP Address and click on Next to continue.

- Name - Enter the RADIUS Server name
- Network Device IP / mask - Enter the Network Devices Hostname or IP Address
- Secret - Enter the RADIUS Secret and confirm
- Type - From the drop down menu select the type of authentication device being used.
- Description - Enter any description necessary.

14. Click Next to complete

15. You have now completed the Setup Wizard, click on Close to exit.

Configuring Network Settings

Any network settings not configured during the Setup Wizard can be setup at any time. To configure remaining network settings follow the steps below:

1. From the administration interface, select Server > Network Settings from the left panel to go to the Network Settings page. This page provides all the network settings that can be changed on FortiConnect as shown below.

Network Settings

Hostname

Hostname: localdomain

Domain:

DNS

Primary DNS:

Secondary DNS:

IPv4

IP Address:

Subnet Mask:

Gateway:

IPv6

Enable: ☐

IP Address:

Prefix Length:

Gateway:

You can change the following Network Settings:

- **Hostname**—Assign the name of the appliance as defined in DNS (without DNS suffix).
- **Domain**—Enter the domain name for your organization (e.g. merunetworks.com).
- **Primary DNS**—Enter the IP address of the primary DNS server.
- **Secondary DNS**—Enter the IP address of the secondary DNS server.

IPv4 Addresses - Enter your IP Address settings for Networks using IPv4

- IP Address—Modify the IP address on the appliance.
- Subnet Mask—Enter the corresponding subnet mask.
- Gateway—Modify the default gateway for the network to which the appliance is connected.

IPv6 Addresses - Click the Enable checkbox if your Network uses IPv6

- IP Address—Modify the IP address on the appliance.
- Prefix Length - From the drop down list select the Prefix Length.
- Gateway—Modify the default gateway for the network to which the appliance is connected.

2. Click the Save button to save the changes that you made.

Note: For any changes of the Network Settings to take effect FortiConnect requires a restart. Clicking Save will initiate the restart process on FortiConnect within 60 seconds.

Date and Time Settings

Correct date and time are critical to FortiConnect as FortiConnect authenticates Users based upon the time their accounts are valid. It is important for the time to be correct so that User accounts are Activated and Expired at the correct time. If possible, Fortinet recommends using a Network Time Protocol (NTP) server to synchronize the time and date.

1. From the administration interface, select Server > Date/Time Settings to display the Date/Time Settings page as shown below.

The screenshot shows the 'Date/Time Settings' window. It has a blue header bar with the title 'Date/Time Settings'. Below the header, there are two main sections: 'Date/Time' and 'NTP'. In the 'Date/Time' section, 'System Date' is set to '1 Dec 2014' with a calendar icon, and 'System Time' is '05:49:47'. 'System Timezone' is set to 'America/Los_Angeles'. The 'NTP' section has a checkbox 'Use NTP to sync System Date & Time' which is currently unchecked. Below this are three input fields for 'NTP Server 1', 'NTP Server 2', and 'NTP Server 3', all containing the address '0.merunetworks.pool.ntp.org'. At the bottom left of the form are 'Save' and 'Cancel' buttons.

2. Select the correct System Date and System Time for the location of your FortiConnect.
3. Select the correct System Timezone for the location of your FortiConnect.
4. Click the Save button to apply any changes.

Note: Changing the System Timezone automatically adjusts the date and time on the FortiConnect appliance and during this time you will be alerted that the change is taking place by a notification -"The application may not respond for a short time while your changes are applied"

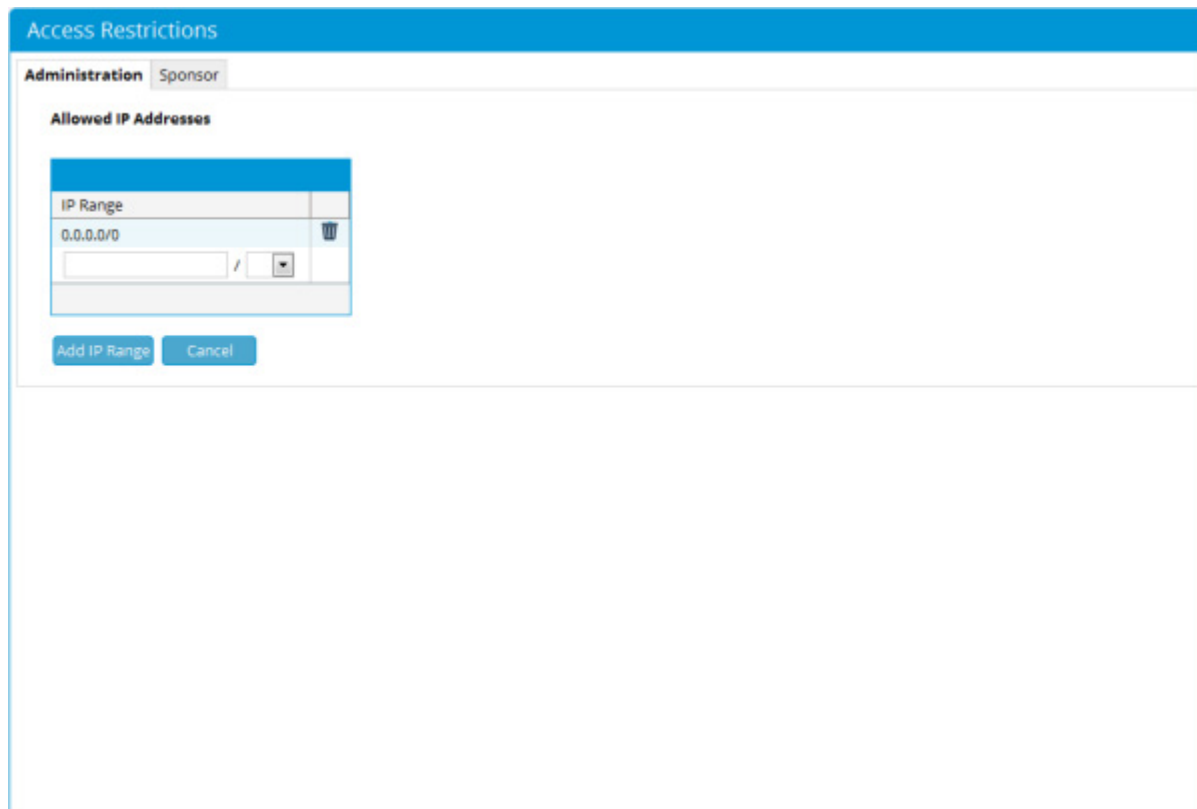
5. If you have one, two or three NTP servers available on the network, click the Use NTP to set System Date & Time checkbox.
6. Enter the IP address of each NTP server available into the fields provided.
7. Upon clicking the Save button, the system will automatically restart the services and start using NTP.

Access Restrictions


You can configure FortiConnect to restrict access to only certain IP address ranges for the administration interface and the sponsor interface at any one time.

Administration Access

1. From the administration interface, select Server > Access Restrictions and click the Administration tab as shown below.



The screenshot shows the 'Access Restrictions' configuration window with the 'Administration' tab selected. The 'Allowed IP Addresses' section contains a table with one entry: '0.0.0.0/0'. Below the table are 'Add IP Range' and 'Cancel' buttons.

IP Range	
0.0.0.0/0	
<input type="text"/>	<input type="text"/> / <input type="text"/>

2. In the Allowed IP Addresses field, type a range of IP addresses that are allowed access to the FortiConnect Administration interface, and apply a CIDR subnet range using the dropdown menu.
3. Click Add IP Range to add the addresses to the list.

Note: Leaving the IP Range field blank allows all IP addresses to access the Administration interface, if users have the required admin account permissions.

Sponsor Access

1. From the administration interface, select Server > Access Restrictions and click the Sponsor tab as shown below.

The screenshot shows the 'Access Restrictions' window with the 'Sponsor' tab selected. The 'Allowed IP Addresses' section contains a table with one row: '0.0.0.0/0'. Below the table are 'Add IP Range' and 'Cancel' buttons.

IP Range	
0.0.0.0/0	
<input type="text"/>	<input type="text"/> / <input type="text"/>

2. Type the range of IP addresses that are allowed to access the Sponsor interface, and apply a CIDR subnet range using the dropdown menu.
3. Click on Add IP Range to add them to the list.

Note: Leaving the IP Range field blank allows all IP addresses to access the Sponsor interface, if users have the required sponsor account permissions.

Configuring SSL Certificates

Both sponsors and administrators can access FortiConnect using either HTTP or HTTPS. For more secure access Fortinet recommends using HTTPS.

This section describes the following:

- Accessing FortiConnect Using HTTP or HTTPS
- Generating Temporary Certificates/CSRs/Private Key
- Downloading Certificate Files
- Uploading Certificate Files

Accessing FortiConnect using HTTP or HTTPS

You can configure whether sponsors and administrators access the portal using HTTP, HTTP and HTTPS, or HTTPS only.

1. From the administration interface, select Server > SSL Settings from the left panel to display the SSL Settings page as shown below.

The screenshot shows the 'SSL Settings' window with the 'HTTP and HTTPS' tab active. The tab bar includes 'Server Certificate', 'Trusted CA Certificates', 'Certificate Revocation Lists', and 'SSL Renegotiation'. The main content area contains four radio button options: 'Allow Only HTTPS', 'Allow Only HTTP', 'Allow HTTPS and HTTP' (selected), and 'Allow Only HTTPS (with HTTP Redirected to HTTPS)'. At the bottom of the content area are 'Save' and 'Cancel' buttons.

2. Click on the HTTP and HTTPS tab and select from one of the following options:
 - **Allow Only HTTPS**—When selected, only allows HTTPS access to the sponsor and administration interfaces of FortiConnect.
 - **Allow Only HTTP**—When selected, only allows HTTP access to the sponsor and administration interfaces of FortiConnect.
 - **Allow HTTPS and HTTP**—When selected, allows both HTTPS and HTTP access to the sponsor and administration interfaces of FortiConnect.
 - **Allow Only HTTPS (with HTTP Redirected to HTTPS)**—When selected, allows sponsors and administrators to access the portal with HTTPS only, however, sponsors and administrators are redirected via HTTPS if using a standard HTTP connection.
3. When you have made your selection, click the Save button.

Generating Temporary Certificates/CSRs/Private Key

FortiConnect generates a default certificate when first installed. If you are planning on using HTTPS, Fortinet strongly recommends generating a new temporary certificate and private key. When doing this, a certificate signing request (CSR) is also generated that can be used to obtain a Certificate Authority (CA) signed certificate.

1. From the administration interface, select Server > SSL Settings from the left hand menu. Select the Server Certificate tab and click the Create CSR link from the section of the page as shown below to bring up the Create CSR form shown below that.

The screenshot displays the 'SSL Settings' interface with the 'Server Certificate' tab selected. The 'Certificate Signing Request' section contains links for 'Create CSR', 'Create Temporary Certificate from CSR', and 'Download CSR'. The 'Download' section has links for 'Download Current SSL Certificate' and 'Download Current SSL Private Key'. The 'Upload Certificate' section includes a file upload field for the 'Server's SSL Certificate'. The 'Upload Certificate and Private Key' section includes separate file upload fields for both the 'Server's SSL Certificate' and the 'Server's SSL Private Key'. At the bottom of the upload section are 'Upload' and 'Cancel' buttons.

Create CSR Form

Create CSR

HTTP and HTTPS **Server Certificate** Trusted CA Certificates Certificate Revocation Lists SSL Renegotiation

CSR

Common Name (FQDN or IP Address):

Organization:

Organizational Unit (Section):

Locality (e.g. City):

State or Province:

Country:

Private Key Regeneration

Warning: If you regenerate your private key your current certificate will be replaced by a self-signed temporary certificate

Regenerate Private Key: ☐

2. Provide the details for the temporary certificate and CSR in the Create CSR form:
 - **Common Name (FQDN or IP Address)**—This is either the IP address of FortiConnect or the fully qualified domain name (FQDN) for the FortiConnect appliance. The FQDN must resolve correctly in DNS.
 - **Organization**—The name of your organization or company.
 - **Organizational Unit (Section)**—The name of the department or business unit that owns the device.
 - **Locality (e.g. City)**—The city where the server is located.
 - **State or Province**—The state where the server is located.
 - **Country**—Select the relevant country from the dropdown menu.
3. The Regenerate Private Key checkbox is optional and should be used if you think your existing private key has been compromised. If you regenerate your private key, the current certificate is invalidated and a new self-signed temporary certificate is generated using the new private key and CSR. Select this option to regenerate a private key.
4. Click Create.

5. The Certificate Signing Request page is again displayed as shown previously. If you chose to regenerate the private key, services will be restarted to enable you to use the new certificate and private key.
6. The Create Temporary Certificate from CSR and Download CSR options are now available as shown below.

The screenshot shows the 'SSL Settings' interface. At the top, a blue header bar contains the text 'SSL Settings'. Below this, a status bar indicates 'CSR Created' with a green checkmark icon. A tabbed interface follows, with 'Server Certificate' selected. Under the 'Certificate Signing Request' section, there are three links: 'Create CSR', 'Create Temporary Certificate from CSR', and 'Download CSR'. Below these links is a 'Download' section with two links: 'Download Current SSL Certificate' and 'Download Current SSL Private Key'. The 'Upload Certificate' section contains a label 'Upload this Server's SSL Certificate:' followed by a 'Choose File' button and the text 'No file chosen'. The 'Upload Certificate and Private Key' section contains two labels: 'Upload this Server's SSL Certificate:' and 'Upload this Server's SSL Private Key:', each followed by a 'Choose File' button and the text 'No file chosen'. At the bottom of this section are 'Upload' and 'Cancel' buttons.

7. Selecting Create Temporary Certificate from CSR generates a temporary certificate from the previously requested Certificate Signing Request that you created in Steps 1 to 4.
8. You can download the CSR by clicking the Download CSR option as shown above. Once you have sent the CSR to a Certificate Authority and obtained the CA-signed certificate in return, you can upload it by following the instructions in the Uploading Certificate Files section.

Note: The installed and generated private keys are 2048 bits in length

Downloading the Certificate

Fortinet strongly recommends backing up the certificate and private key. The certificate can be downloaded from the administration interface for manual backup to a secure location.

1. From the administration interface, select Server > SSL Settings from the left hand menu. Open the Server Certificate tab
2. Select Download Current SSL Certificate from the Download Certificate section of the page as shown below.

The screenshot displays the 'SSL Settings' page in the Fortinet administration interface. The 'Server Certificate' tab is selected. The page is divided into several sections:

- Certificate Signing Request:** Contains links for [Create CSR](#), [Create Temporary Certificate from CSR](#), and [Download CSR](#).
- Download:** Contains links for [Download Current SSL Certificate](#) and [Download Current SSL Private Key](#).
- Upload Certificate:** Includes a label 'Upload this Server's SSL Certificate:' followed by a 'Choose File' button and the text 'No file chosen'.
- Upload Certificate and Private Key:** Includes two labels: 'Upload this Server's SSL Certificate:' and 'Upload this Server's SSL Private Key:'. Each is followed by a 'Choose File' button and the text 'No file chosen'.

At the bottom of the form, there are two buttons: 'Upload' and 'Cancel'.

3. Save the SSL Certificate to a secure backup location.

Uploading Certificate and Private Key Files

FortiConnect provides a method of importing/uploading certificate files to the appliance. The Upload Certificates option is used to install a CA-signed certificate or to restore Base 64 PEM format certificate files previously backed up.

NOTE: You must upload certificate files in Base 64 PEM format or DER format. The certificate files are not backed up as part of any backup process. You must manually back them up as described in [Downloading Certificate Files](#)

1. From the administration interface, select Server > SSL Settings from the left hand menu. Select the Server Certificate tab.
2. View the Upload Certificates section at the bottom of the page as shown below.

The screenshot displays the 'SSL Settings' page with the 'Server Certificate' tab selected. It features several sections: 'Certificate Signing Request' with links for 'Create CSR', 'Create Temporary Certificate from CSR', and 'Download CSR'; a 'Download' section with links for 'Download Current SSL Certificate' and 'Download Current SSL Private Key'; and an 'Upload Certificate' section. The 'Upload Certificate' section contains two rows: one for 'Upload this Server's SSL Certificate' and another for 'Upload this Server's SSL Private Key'. Each row has a 'Choose File' button and the text 'No file chosen'. At the bottom of the 'Upload Certificate' section are 'Upload' and 'Cancel' buttons.

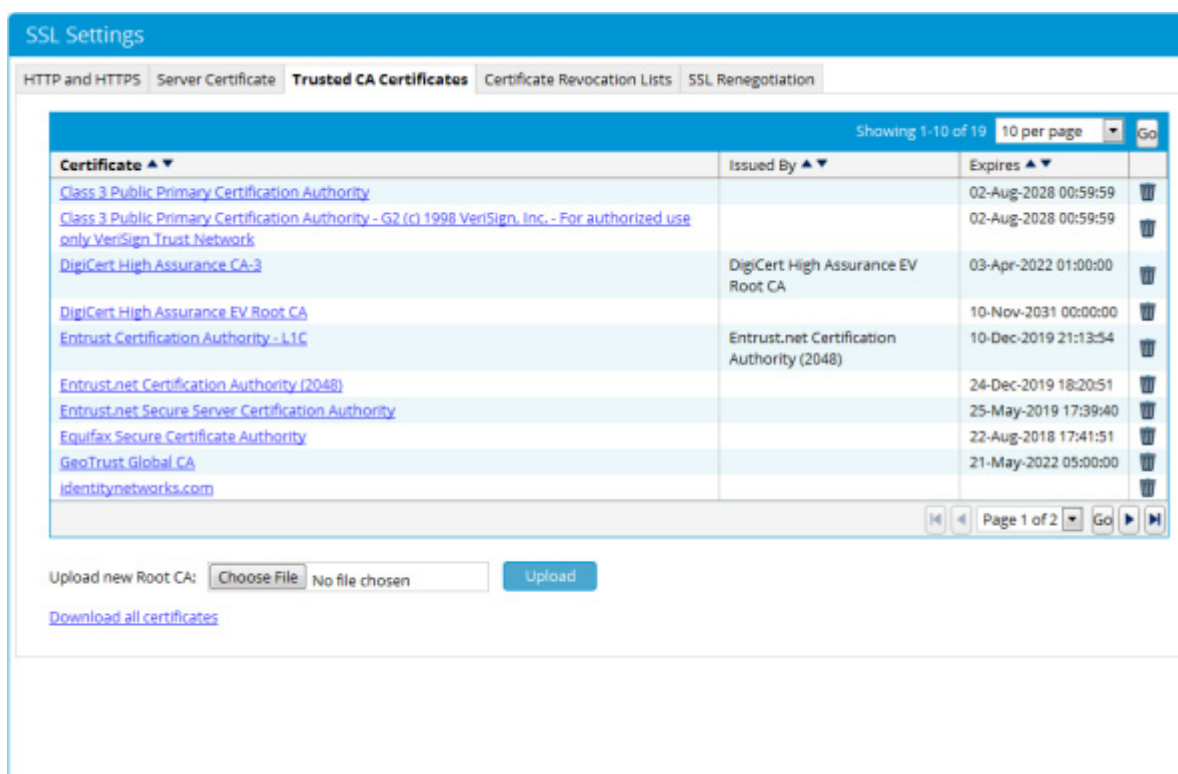
3. Click the Choose File button to locate the SSL Certificate file you want to upload and click the Upload button.
4. If the private key have been created separately, then you can select them both from different locations and upload them under the Upload Certificate and Private Key section on the same page.

WARNING -When uploading a certificate, it must match the private key installed.

Uploading Trusted CA Certificates

FortiConnect allows you to upload Trusted CA Certificates so that it can trust devices that it makes SSL connections to.

1. From the FortiConnect interface select Server > SSL Settings and click on the Trusted CA Certificates tab as below.



2. Click on the Choose File button next to the Upload new Root CA option and click on the upload button once you have selected the desired Certificate to upload.
3. You can also click on the Download All Certificates link to download all certificates.

Certificate Revocation Lists

A certificate is irreversibly revoked if, for example, it is discovered that the Certificate Authority (CA) had improperly issued a certificate, or if a private-key is thought to have been compromised. Certificates may also be revoked for failure of the identified entity to adhere to policy requirements such as publication of false documents, mis-representation of software behavior, or violation of any other policy specified by the CA operator or its customer. The most common reason for revocation is the user no longer being in sole possession of the private key (*e.g.*, the token containing the private key has been lost or stolen).

FortiConnect automatically uploads Trusted Certificates to a Revocation List and updates the Certificate at a set specific time period to ensure the Certificate is still valid.

1. The list can be viewed by navigating to Server --> SSL Settings and then clicking on the Certificate Revocation List tab on the FortiConnect Administration database as shown below.

SSL Settings

HTTP and HTTPS | Server Certificate | Trusted CA Certificates | **Certificate Revocation Lists** | SSL Renegotiation

CRLs are checked when Sponsors or Network Users authenticate using Client Certificates. For security reasons the web service will be stopped if a downloaded CRL expires, this can occur if the Meru Connect does not have internet access.

10 per page Go

URL ▲▼	Last Update ▲▼	Next Update ▲▼	Status ▲▼
No CRLs installed			

New CRL:

URL e.g. http://your.server.com/crl

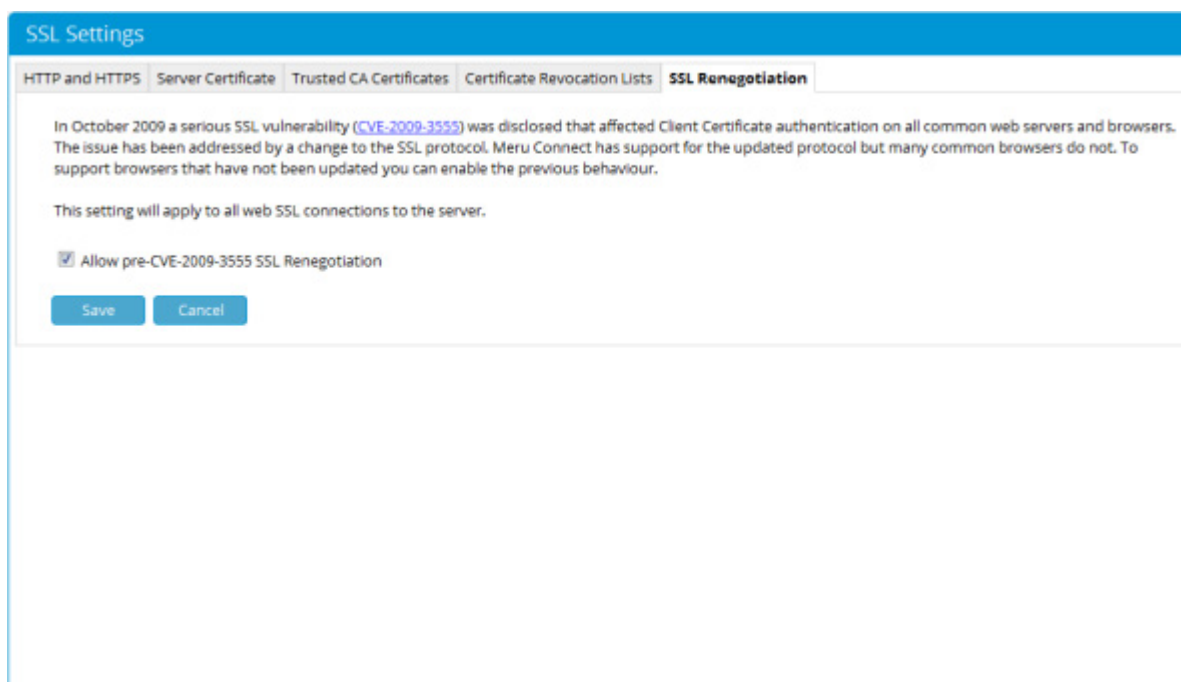
Update Every: minutes

2. CRL's can be manually added to this list by entering the URL of the stored CRL into the New CRL box.
3. Enter a time value that you wish this CRL to be updated and then click on the Add button to add this to the list.

SSL Renegotiation

In October 2009 a serious SSL vulnerability (CVE-2009-3555) was disclosed that affected Client Certificate authentication on all common web server and browsers. The issue has been addressed by a change to the SSL protocol. FortiConnect has support for the updated protocol but many common browsers do not. To support browsers that have not been updated you can enable the previous behaviour.

From the FortiConnect Administration Interface go to Server --> SSL Settings and click on the SSL Renegotiation tab as shown below.



Click on the Allow pre-CVE-2009-3555 SSL Renegotiation box to enable renegotiation. This setting will apply to all web SSL connections to the server.

Configuring Administrator Authentication

FortiConnect has a single default administrator account, called “admin.” The Admin Accounts pages under the Authentication menu allow you to create, edit and delete additional administrator accounts. You can additionally configure FortiConnect to authenticate administrators against an external RADIUS server.

This section describes the following:

- Add New Admin Account
- Edit Existing Admin Account
- Delete Existing Admin Account
- Admin Session Timeout
- Configuring RADIUS for Administrator Authentication

Add New Admin Account

1. From the administration interface, select Server > Admin Users from the left hand menu.
2. In the Local Database tab of the Administrators page as shown below, click the Add Administrator button.

Add New Admin Account

Admin Users

Local Database

RADIUS Authentication

Username	First Name	Last Name	Email	Group	
admin	admin	user	admin@a.com	Full Access	
editor	J	J	j@a.com	Portal Manager	

Add

3. In the Add Administrator page as shown below, enter all the admin user credentials.

Add Administrator

Username:

First Name:

Last Name:

Email:

Password: Confirm:

Your password must be at least six characters long and contain a minimum of four different characters

Group:

- First Name—Type the first name of the admin user
- Surname—Type the last name of the admin user.
- Email —Type the email address of the admin user
- Username—Type the user name for the admin account.
- Password—Type the password for the admin account.
- Confirm—Retype the password for the admin account

Note: The password must be at least six characters long and contain at least four different characters

- Group - from the drop down menu add your Admin to a group based on access permissions -
 - ⑧ Full access - Full Administration access
 - ⑧ Portal Manager - can only see Portal, Portal Rules, Themes and Hosted Files entries.
 - ⑧ Portal Content Editor - can only edit portal text, images and colours.

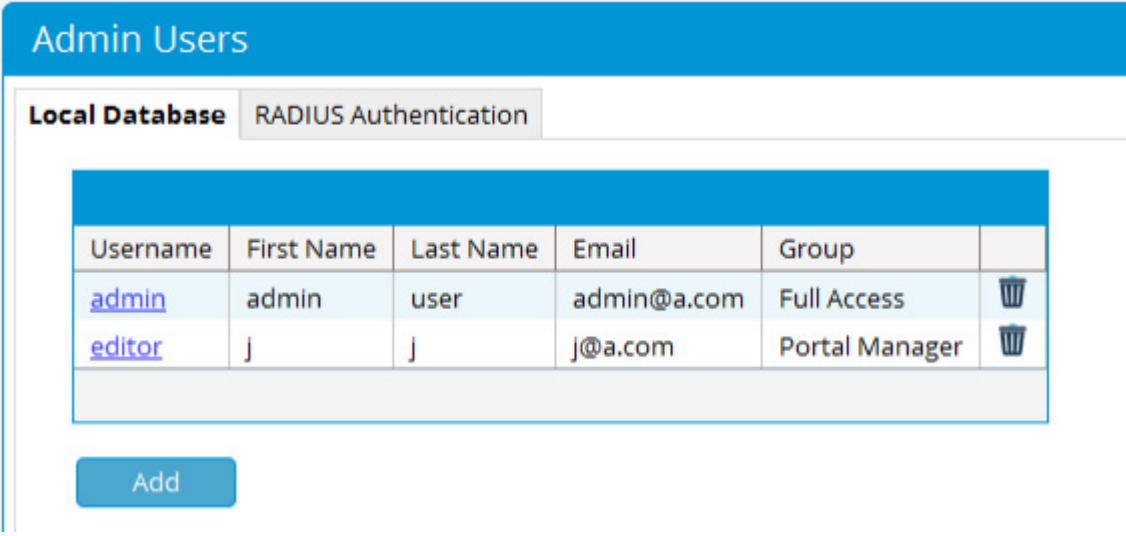
4. Click the Add button.

- If there are any errors, the account is not added and an error message is displayed at the top of the page.
- If successfully added, a success message is displayed at the top of the page and you can add additional admin accounts.

Edit Existing Admin Account



You can modify the settings of admin accounts that already exist.

1. From the administration interface, select **Server > Admin users** from the left hand menu.
2. In the **Local Database** tab of the **Administrators** page as shown below, click the username from the list.



Admin Users

Local Database | RADIUS Authentication

Username	First Name	Last Name	Email	Group	
admin	admin	user	admin@a.com	Full Access	
editor	j	j	j@a.com	Portal Manager	

[Add](#)

3. In the **Edit Administrator** page as shown below, edit the user credentials.

Edit Administrator

Username: admin

First Name:

Last Name:

Email:

Password: Confirm:

Leave blank to keep existing password

Group:

- First Name—Edit the first name of the admin user
- Surname—Edit the last name of the admin user.
- Email —Edit the email address of the admin user
- Password—Edit the password for the admin account.
- Confirm—Edit the password for the admin account.
- Group - from the drop down menu add your Admin to a group based on access permissions -
 - ⑧ Full access - Full Administration access
 - ⑧ Portal Manager - can only see Portal, Portal Rules, Themes and Hosted Files entries.
 - ⑧ Portal Content Editor - can only edit portal text, images and colours.

Note: Leaving the Password and Confirm Password fields empty keeps the existing password.

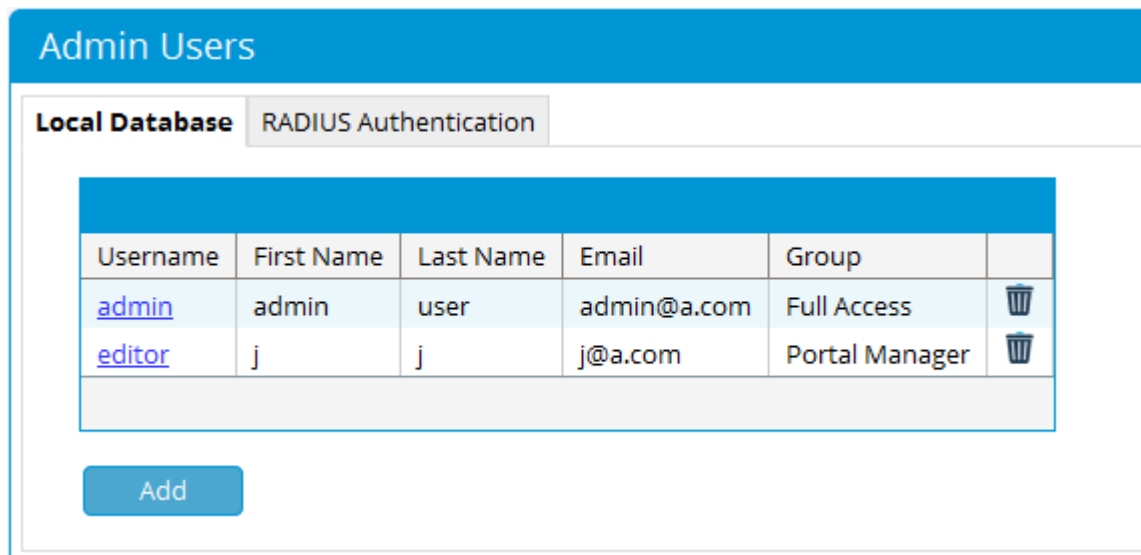
4. Click the Save Settings button.

- If there are any errors, the account is not changed and an error message is displayed at the top of the page.
- If successfully changed, a success message is displayed at the top of the page and you can make additional changes to the same admin account.

Delete Existing Admin Account

You can remove existing admin accounts from the administration interface.

1. From the administration interface, select **Server > Admin Users** from the left hand menu.



2. In the Admin Accounts page as shown above, click the bin icon at the end of the user entry that you want to delete.
3. When prompted, click OK to delete the user or Cancel to cancel the deletion. If successfully deleted, a success message is displayed at the top of the page.

Configuring RADIUS for Administrator Authentication

As an alternative to configuring local administrator accounts, you can configure admin users to be authenticated over RADIUS to a RADIUS server. To configure RADIUS authentication for Administrator Authentication, perform the following steps:

1. From the administration interface, select Server > Admin Users.
2. Click the RADIUS Authentication tab as shown below.

Admin Users

Local Database **RADIUS Authentication**

Meru Connect only allows access to admin users authenticating against a RADIUS server when the RADIUS server returns the IETF Service-Type attribute set to 6 (administrative) as part of the Access-Accept Message.

Primary Server

Server IP Address:

Port:

RADIUS Secret: Confirm:

Leave blank to keep existing secret

Secondary Server

Server IP Address:

Port:

RADIUS Secret: Confirm:

Group

Users will be placed in this group when authenticated.

Group:

Authentication Mode

Only allow local user authentication if both RADIUS servers cannot be contacted: ☐

3. Type the Server IP Address for the Primary RADIUS Server.
4. Type the Port that RADIUS authentication is running on for that server (default is 1645 or 1812).
5. In the RADIUS Secret field, type the shared secret to be used between the RADIUS Server and FortiConnect.
6. Confirm the secret to make sure that it is set correctly.
7. Enter details for a Secondary RADIUS Server. These details are used when FortiConnect does not receive a response from the Primary RADIUS Server. These fields are optional.
8. Group - from the drop down menu add your Admin to a group based on access permissions -
 - Ⓢ Full access - Full Administration access
 - Ⓢ Portal Manager - can only see Portal, Portal Rules, Themes and Hosted Files entries.
 - Ⓢ Portal Content Editor - can only edit portal text, images and colours.

9. Check the Authentication Mode checkbox so that Local Admin account is only allowed if both the RADIUS Servers cannot be contacted. If this option is unchecked, Local Admin account is allowed if authentication is denied for any one of the RADIUS Servers.
10. Click the Save button to save the Administrator RADIUS settings.

Note: FortiConnect only allows access to admin users who are successfully authenticated. The RADIUS server must return the IETF Service-Type attribute set to 6 (administrative).

Configuring TACACS+ for Administrator Authentication

Admin authentication can be configured with TACACS+ server. Authentication Type can be None, TACACS+ or RADIUS.

Select None if no external authentication (RADIUS or TACACS+) is used and Admin will be authenticated against the local FortiConnect database.

Select TACACS+ is selected, you must specify a primary server and secondary server. Secondary server will be used if Primary server is not reachable/unable to connect.

Default port number is 49 and Secret can be any string which matches the Secret configured in TACACS+ server. FortiConnect should be added as AAA client in TACACS+ server. Only PAP mode authentication is supported.

The screenshot shows the 'Admin Users' configuration page in FortiConnect, specifically the 'External Authentication' tab. The left sidebar contains a navigation menu with the following items: HOME, NETWORK ACCESS POLICY, POLICY SETTINGS, SPONSOR PORTAL, GUEST PORTALS, SMART CONNECT, DEVICES, REPORTS & LOGS, and SERVER. Under the 'SERVER' category, 'Admin Users' is selected and highlighted in blue. Below it are 'Interface Timeout', 'Network Settings', 'Date/Time Settings', and 'Access Restrictions'. The main content area is titled 'Admin Users' and has two tabs: 'Local Database' and 'External Authentication'. The 'External Authentication' tab is active. It contains the following fields: 'Authentication Type' (a dropdown menu with 'TACACS+' selected and highlighted by a red box, with other options 'None' and 'Radius' visible), 'Primary Server' (a section header), 'Server IP Address' (text input: 172.18.1.5), 'Port' (text input: 49), 'Secret' (text input) and 'Confirm' (text input) fields, with a note 'Leave blank to keep existing secret' below the 'Secret' field. Below this is the 'Secondary Server' section with similar fields for IP Address, Port, Secret, and Confirm. At the bottom is the 'Group' section with the text 'Users will be placed in this group when authenticated.' and a 'Group' dropdown menu set to 'Full Access'. The 'Authentication Mode' section is partially visible at the bottom.

Data Retention

FortiConnect allows you to delete or archive old data from the system, to configure the settings from the administration interface go to Server-->Data Retention, you will see the screen below.

Data Retention

Settings | Schedule

Enable: ☒

Process data older than: 1 Days

Policy: Delete only

Server:

Port:

Passive Mode: ☒

Directory:

Username:

Password: Confirm:

Save Cancel Process Now

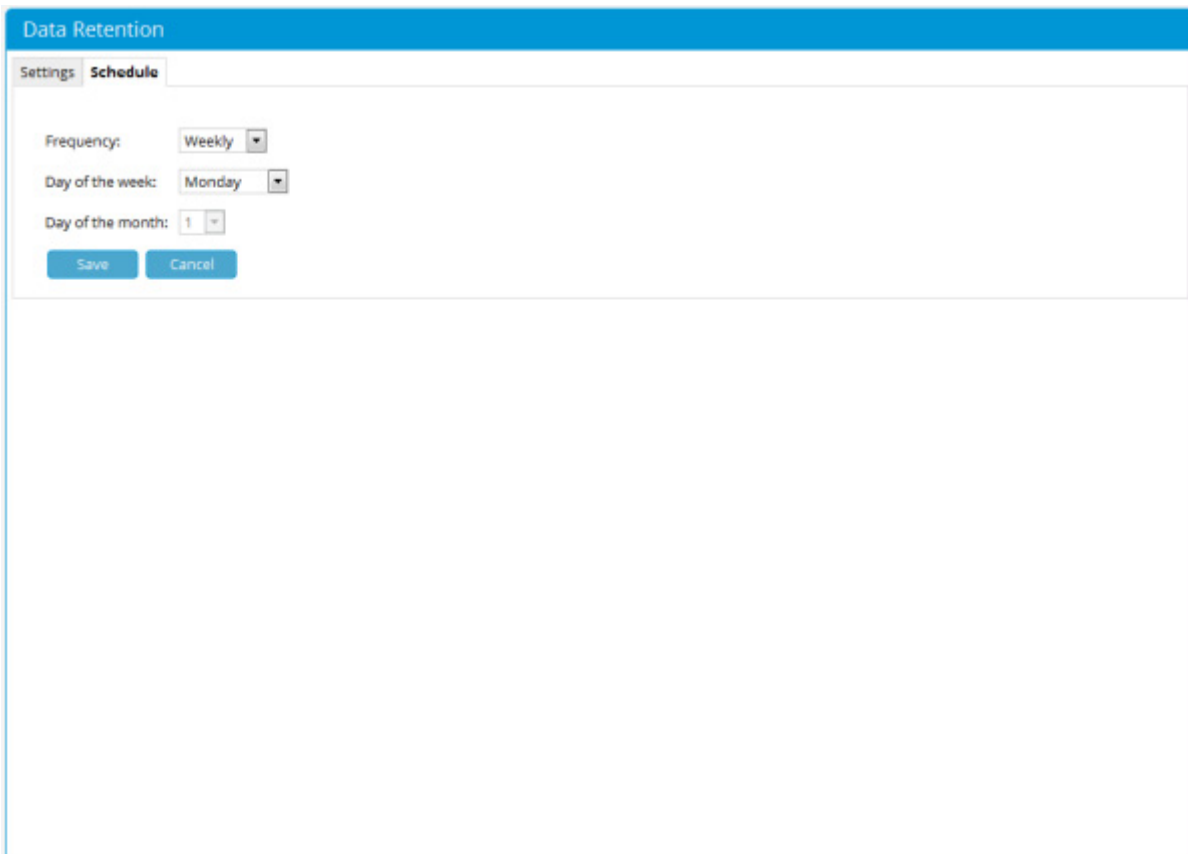
Unused Accounts

Expire inactive for: 0 Days This applies to all accounts

Process Unused Accounts

1. Click on the Settings tab to set the archive details :-
 - Place a check in the Enable check box to enable Data Retention.
 - In the Process data older than fields use the drop down menu to select whether you wish to process data in days, weeks, months or years, then enter your desired figure into the field next to it.
 - From the Policy drop down menu select whether you wish to Delete only (no further action in this section will be needed) or whether you wish to Archive to FTP and delete, or Archive to SFTP and delete.
2. If you have selected to FTP or SFTP you will be required to enter further information :-
 - In the Server field, enter the IP address or hostname of your server.
 - In the Port field, enter the required port number.
 - in the Directory field, enter the required directory.
 - In the Username field, enter the required Username
 - In the Password field, enter the required Password and then enter again to Confirm.
3. Click on Save to save your settings, or click on Process Now to start the process immediately.
4. You can expire any Unused Accounts if they have been inactive for a certain amount of time.

- From the drop down menu, choose from years, days, hours or minutes.
 - Enter a specified time in the Expire inactive for field
 - Click on Process Unused Accounts
5. To configure the schedule from the administration interface go to Server-->Data Retention, you will see the screen below.



The screenshot shows a web interface titled "Data Retention". It has two tabs: "Settings" and "Schedule", with "Schedule" being the active tab. The "Schedule" tab contains three configuration fields: "Frequency" with a dropdown menu set to "Weekly", "Day of the week" with a dropdown menu set to "Monday", and "Day of the month" with a dropdown menu set to "1". Below these fields are two buttons: "Save" and "Cancel".

6. Click on the Schedule tab to set the schedule details :-
- From the Frequency drop down menu, select whether the schedule should run Daily, Weekly or Monthly.
 - If necessary, from the Day of the week drop down menu, select what day of the week the schedule should run.
 - If necessary, from the Day of the month drop down menu, select what day of the month the schedule should run.

Configuring Sponsor Authentication

Sponsors are the people who use FortiConnect to create User accounts.

Sponsor authentication authenticates those sponsor users to the Sponsor interface of FortiConnect. There are five options available:

- Local User Authentication—Create local sponsor accounts directly on FortiConnect. See [Configuring Local Sponsor Authentication](#).
- Active Directory Authentication—Authenticate sponsors against an existing Active Directory (AD) infrastructure. See [Configuring Active Directory \(AD\) Authentication](#).
- LDAP Authentication—Authenticate sponsors against a Lightweight Directory Access Protocol (LDAP) server. See [Configuring LDAP Authentication](#).
- Novell eDirectory - Authenticate sponsors against a Novell eDirectory server. See [Configuring Novell eDirectory](#).
- RADIUS Authentication—Authenticate sponsors against a RADIUS server. See [Configuring RADIUS Authentication](#).
- Active Directory Single Sign-On—This option uses Kerberos between the client's web browser and FortiConnect to automatically authenticate a sponsor against an Active Directory Domain Controller. See [Configuring Active Directory Single Sign-On](#).
- Client Certificate Authentication - This option allows a sponsor to present a certificate through their browser to authenticate themselves. Once this has been done the sponsor can be mapped to a role based upon an LDAP server.

You can configure multiple authentication servers in FortiConnect as well as the order in which the authentication servers are used to authenticate sponsors. For details, see [Configuring Sponsor Authentication Settings](#).

Configuring Local Sponsor Authentication

Local authentication allows you to set up sponsor user accounts directly on FortiConnect. You can do the following with local authentication:

- Add New Local User Account
- Edit Existing User Account
- Delete Existing User Account

Add New Local User Account

1. From the administration interface, select Sponsor Portal > Authentication and then click on the Internal Sponsors tab from the menu as shown below.

The screenshot shows the 'Authentication' section of the Fortinet Administration interface. The 'Internal Sponsors' tab is selected. A table displays the following data:

Username ▲▼	First name ▲▼	Last name ▲▼	Email ▲▼	Group ▲▼	
local	local	sponsor	local@idm.com	DEFAULT	

Below the table, there is a pagination bar showing 'Showing 1-1 of 1' and '10 per page'. At the bottom of the section is an 'Add User' button.

2. Click the Add User button to bring up the local sponsor configuration page as shown below.

Add User

Username:

Password: Confirm:

Your password must be at least six characters long and contain a minimum of four different characters

First Name:

Last Name:

Email:

Group:

3. In the Add a Local User Account page, enter all the sponsor user credentials:

- Username - Type the sponsors username.
- Password - Enter the sponsors password.
- Confirm - Confirm the sponsors password.

Note: The password must be at least six characters and must contain at least four different characters

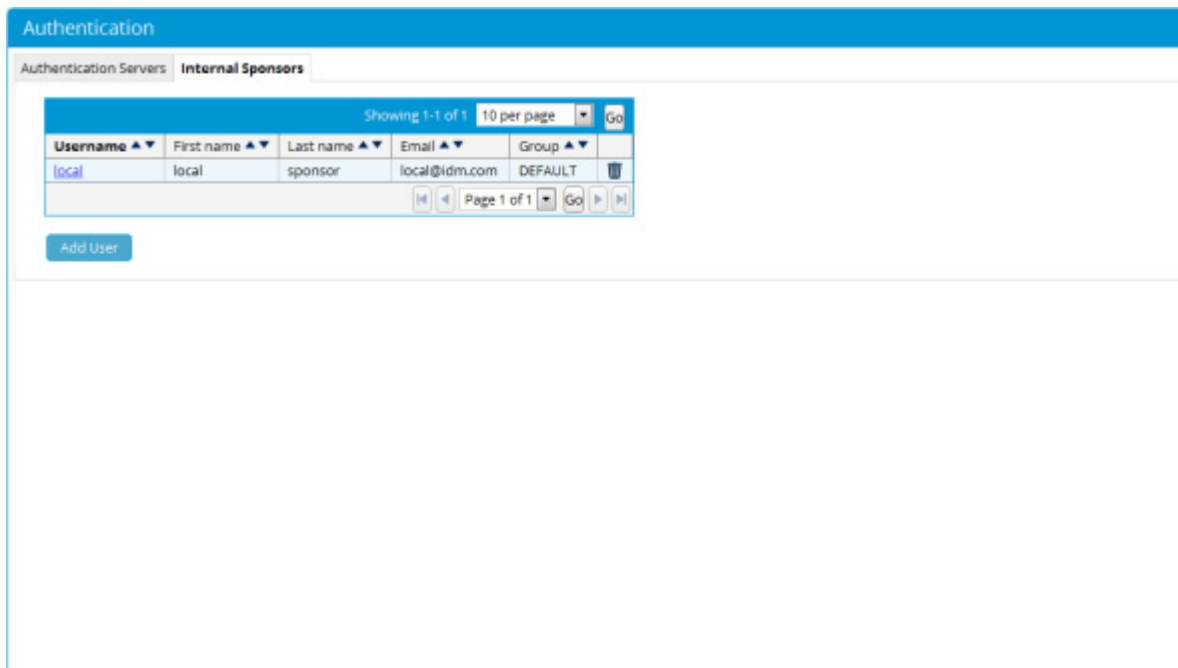
- First Name—Type the first name of the sponsor.
- Last Name—Type the last name of the sponsor.
- Email —Type email address of the sponsor.
- Group—Select the group for the sponsor account from the dropdown.

4. Click the Save button.

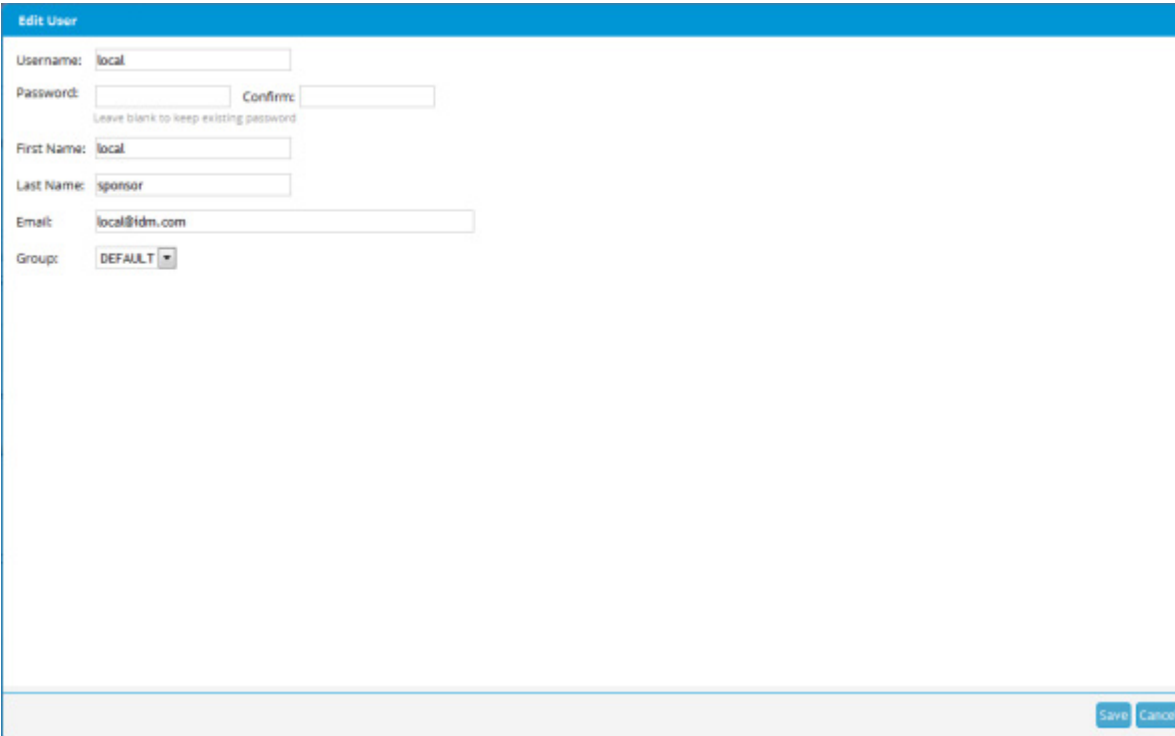
- If there are any errors, the account is not added and an error message is displayed at the top of the page.
- If successfully added, a success message is displayed at the top of the page and you can add additional user accounts.

Edit Existing User Account

1. From the administration interface, select Sponsor Portal > Authentication and then click on the Internal Sponsors tab from the menu as shown below.



2. Click on the link of the sponsor you wish to edit, this will bring up the Edit User page as shown below.



Edit User

Username:

Password: Confirm:
Leave blank to keep existing password

First Name:

Last Name:

Email:

Group:

3. In the Edit User page, enter all the sponsor user credentials:

- Username - Type the sponsors username.
- Password - Enter the sponsors password.
- Confirm - Confirm the sponsors password.

Note: Leave passwords blank to retain current password.

- First Name—Type the first name of the sponsor.
- Last Name—Type the last name of the sponsor.
- Email —Type email address of the sponsor.
- Group—Select the group for the sponsor account from the dropdown.

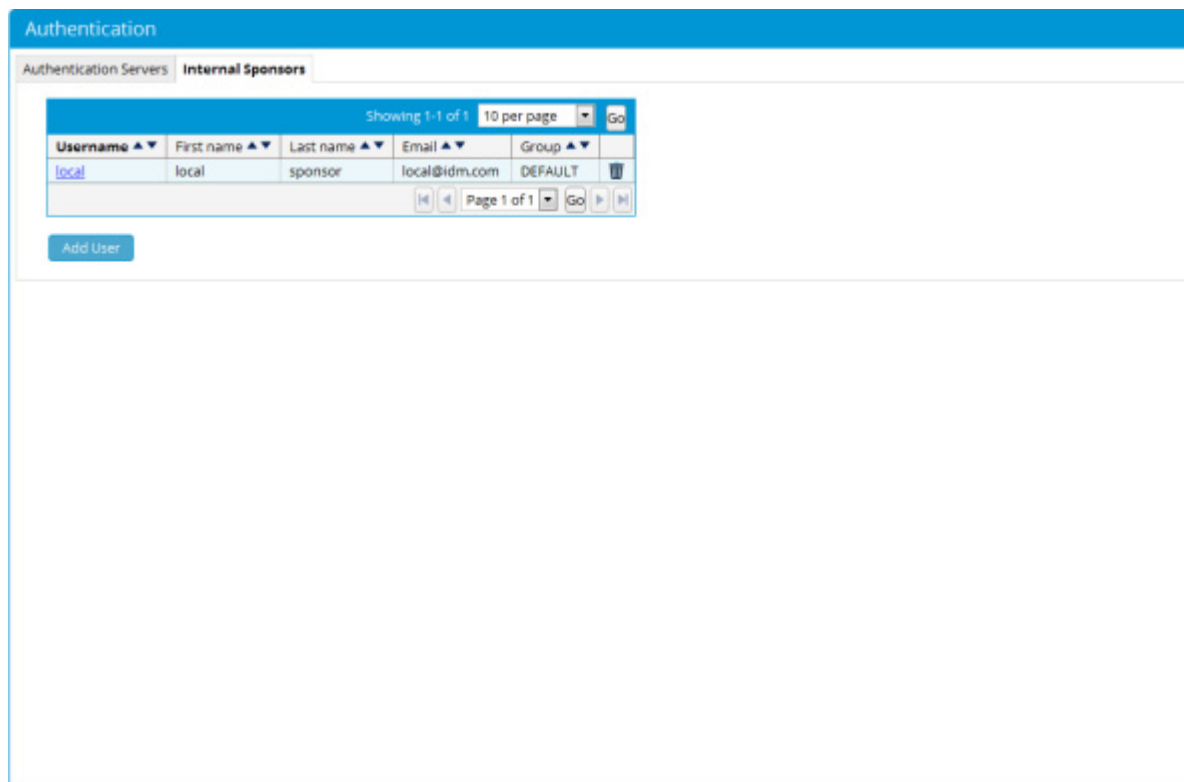
4. Click the **Save** button.

- If there are any errors, the account is not added and an error message is displayed at the top of the page.
- If successfully added, a success message is displayed at the top of the page and you can add additional user accounts.

Delete Existing User Account

You can delete existing sponsor user accounts from the administration interface.

1. From the administration interface, select **Sponsor Portal > Authentication** and then click on the **Internal Sponsors** tab from the menu as shown below.



2. A list of local users appears on the page. Choose the user you wish to delete by clicking the dustbin icon to the right of the Group field.
3. Confirm deletion of the user at the prompt.
 - If successfully deleted, a success message is displayed at the top of the page and you can perform additional local user account operations.

Configuring Active Directory (AD) Authentication

Active Directory authentication authenticates sponsor users to FortiConnect using their existing AD user accounts. The sponsors need not have another set of user names and passwords to authenticate to the FortiConnect appliance. It also enables the administrator to quickly roll out User Access because there is no need to create and manage additional local sponsor accounts.

Active Directory authentication allows you to do the following:

- Add Active Directory Domain Controller
- Edit Existing Domain Controller
- Delete Existing Domain Controller Entry

AD authentication supports authentication against multiple domain controllers. The domain controllers can be part of the same Active Directory to provide resilience, or they can be in different Active Directories. FortiConnect can authenticate sponsor users from separate domains, even where no trust relationship is configured.

All Active Directory authentication are performed against individual domain controller entries.

FortiConnect attempts to authenticate sponsors against each Domain Controller entry according to the Authentication Order (specified in Configuring Sponsor Authentication Settings).

Note: If below security settings are present in Domain Controller Security

Domain controller: LDAP server signing requirements - Set to "Require Signing"

Network security: LDAP client signing requirements - Set to "Negotiate signing" or "Require signing"

Then the encryption type for the AD Server in MCT should not be "None".

Add Active Directory Domain Controller

1. From the administration interface, select Sponsor Portal > Authentication. Select the Authentication Servers tab below.

Add Active Directory Domain Controller

Authentication

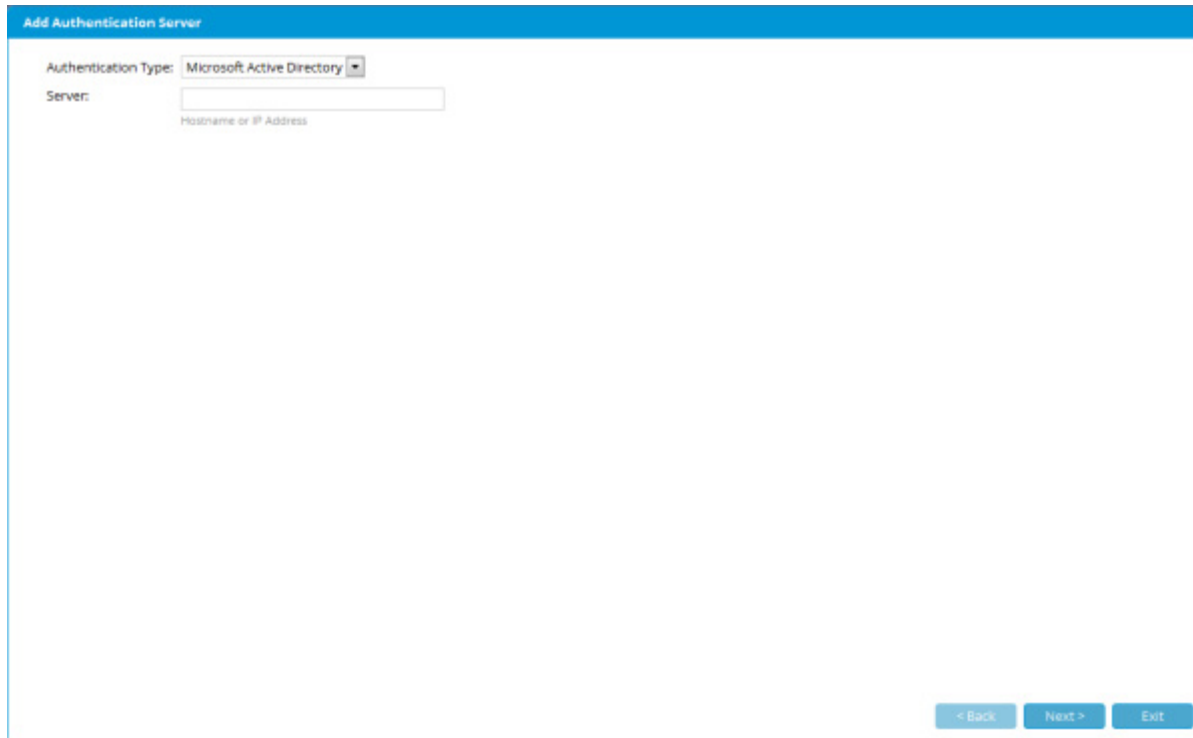
Authentication Servers Internal Sponsors

When a Sponsor attempts to log in their credentials are tested against these servers in order until an authentication attempt succeeds. However if a browser supplies a Client Certificate or Single Sign On credentials these are checked before any other authentication methods.

Order	Enabled	Name	Type	Server	Client Certificates	Single Sign On
1		Local	Internal sponsor database	n/a	n/a	n/a

Add Server...Save OrderCancel

2. Click the Add Server button.
3. From the Authentication type drop down menu, select Microsoft Active Directory
4. In the Server text box insert the Hostname or IP address of the AD server as shown below.



Add Authentication Server

Authentication Type: Microsoft Active Directory

Server:

Hostname or IP Address

< Back Next > Exit

Enter details required as shown in the screenshot below.

- Name—Type a text description of the Server Name or IP Address.
- Server Type - Will auto populate with the server type.
- Server - Will auto populate with the servers IP address.
- Domain - Will auto populate with the system domain.
- Encryption - From the drop down menu, select the desired encryption method.
- Base DN— From the drop down menu, select the Base Distinguished Name (DN) of the domain controller. This is the name of the root of the directory tree. It is used so that when group searches are performed, the FortiConnect knows from where to start. An example of the base DN for the domain cca. identitynetworks.com is DC=cca,DC=identitynetworks,DC=com.

Add Active Directory Domain Controller

Add Authentication Server

Name: 10.10.1.2

Server Type: Microsoft Active Directory

Server: 10.10.1.2

Domain: identitynetworks.com

Encryption: None

This server supports encryption, but its certificate cannot be validated. You must upload its certificate or its root certificate to continue:

Certificate: Choose File No file chosen

Base DN: DC=identitynetworks,DC=com [server default]

< Back Next > Exit

Click on Next and then Enter details required as shown below.

- Username—Type a username that has permissions to search the Active Directory using LDAP. This allows FortiConnect to find out details about users such as the list of groups to which they belong.
- Password—In addition to the AD Username, type the password for that account.
- Confirm— Retype the password for confirmation.

Add Authentication Server

Connection

Name: 10.10.1.2
Server Type: Microsoft Active Directory
Server: 10.10.1.2
Domain: identitynetworks.com
Encryption: None
Base DN: DC=identitynetworks,DC=com

Search Credentials

Username: @identitynetworks.com
Password:

< Back Next > Exit

Click on next to complete.

Once the above details have been entered you can enable/disable the server by clicking on the circle underneath the Enabled column.

Edit Existing Domain Controller

1. From the administration interface, select Sponsor Portal > Authentication and click on the Authentication Servers tab from the menu.
2. Select the Active Directory Domain Controller from the list and click the underlined domain name to select and edit the domain controller as shown below.

Edit Existing Domain Controller

The screenshot shows the 'Authentication' section with the 'Authentication Servers' tab selected. A descriptive paragraph explains the authentication process. Below is a table listing two servers: '10.10.1.2' (Microsoft Active Directory) and 'Local' (Internal sponsor database). The first server is selected, and its details are visible in the table. At the bottom are buttons for 'Add Server...', 'Save Order', and 'Cancel'.

Order	Enabled	Name	Type	Server	Client Certificates	Single Sign On	
1	<input checked="" type="checkbox"/>	10.10.1.2	Microsoft Active Directory	10.10.1.2	Configure	Configure	
2	<input checked="" type="checkbox"/>	Local	Internal sponsor database		n/a	n/a	

3. In the Edit Active Directory Domain Controller page as shown in the screenshot below, edit the details for authenticating against this AD domain controller

The screenshot shows the 'Edit Authentication Server' page. It contains fields for Name, Server Type, Server, Domain, Encryption, Certificate, and Base DN. The 'Name' field is highlighted. A warning message states: 'This server supports encryption, but its certificate cannot be validated. You must upload its certificate or its root certificate to continue:'. At the bottom are buttons for '< Back', 'Next >', and 'Exit'.

Name: 10.10.1.2

Server Type: Microsoft Active Directory

Server: 10.10.1.2

Domain: identitynetworks.com

Encryption: None

This server supports encryption, but its certificate cannot be validated. You must upload its certificate or its root certificate to continue:

Certificate: Choose File No file chosen

Base DN: DC=identitynetworks,DC=com [server default]

4. Modify settings as needed:
 - Name - Type a text description of the Server Name or IP Address.
 - Server Type - Will auto populate with the server type.

- Server - Will auto populate with the servers IP address.
- Domain - Will auto populate with the system domain.
- Encryption - From the drop down menu, select the desired encryption method.
- Base DN - From the drop down menu, select the Base Distinguished Name (DN) of the domain controller. This is the name of the root of the directory tree. It is used so that when group searches are performed, FortiConnect knows from where to start. An example of the base DN for the domain cca. merunetworks.com is DC=cca,DC=merunetworks,DC=com.

Click on next and edit search credentials, below.

Edit Authentication Server

Connection

Name: 10.10.1.2
 Server Type: Microsoft Active Directory
 Server: 10.10.1.2
 Domain: identitynetworks.com
 Encryption: None
 Base DN: DC=identitynetworks,DC=com

Search Credentials

Username: administrator @identitynetworks.com
 Password: Leave blank to keep existing password

< Back Next > Exit

- Username - Type a username that has permissions to search the Active Directory using LDAP. This allows FortiConnect to find out details about users such as the list of groups to which they belong.
- Password - In addition to the AD Username, type the password for that account.
- Confirm - Retype the password for confirmation

Click on Next to finish

Once the above details have been entered you can enable/disable the server by clicking on the circle underneath the Enabled column.

Delete Existing Domain Controller Entry

1. From the administration interface, select Sponsor Portal > Authentication from the menu and click on the Authentication Servers tab.
2. Click the underlined name of the domain controller from the list as shown below.

Authentication

Authentication Servers Internal Sponsors

When a Sponsor attempts to log in their credentials are tested against these servers in order until an authentication attempt succeeds. However if a browser supplies a Client Certificate or Single Sign On credentials these are checked before any other authentication methods.

Order	Enabled	Name	Type	Server	Client Certificates	Single Sign On
1 ▼	●	<u>10.10.1.2</u>	Microsoft Active Directory	10.10.1.2	Configure	Configure
2 ▲	●	<u>Local</u>	Internal sponsor database	n/a	n/a	n/a

[Add Server...](#) [Save Order](#) [Cancel](#)

3. Delete the domain controller by clicking the bin icon to the right of the Enabled field.
4. Confirm deletion of the Domain Controller at the prompt.

Configuring LDAP Authentication

LDAP authentication allows FortiConnect to authenticate sponsor users using their existing LDAP user accounts. The sponsors need not have another set of user names and passwords to authenticate to FortiConnect. It also enables the administrator to quickly roll out User Access because there is no need to create and manage additional local sponsor accounts. LDAP authentication allows you to do the following:

- Add an LDAP Server
- Edit an Existing LDAP Server
- Delete an Existing LDAP Server Entry

LDAP authentication supports authentication against multiple LDAP Servers. An LDAP server entry consists of multiple items:

- LDAP Server Name—A text description to identify the LDAP Server.
- LDAP Server URL—This is the URL to access the LDAP server such as `ldap://ldap.merunetworks.com`.
- Base DN—This is the Distinguished Name of the container object where an LDAP search to find the user begins, such as `OU=Engineering,O=merunetworks`.
- User Search Filter—The User Search Filter defines how user entries are named in the LDAP server. For example, you can define them as `uid (uid=%USERNAME%)` or `cn (cn=% USERNAME%)`.
- Group Mapping—There are two main methods that LDAP servers use for assigning users to groups:

Storing the group membership in an attribute of the user object. With this method, the user object has one or more attributes that list the groups to which the user belongs. If your LDAP server uses this method of storing group membership, you need to enter the name of the attribute which holds the groups of which the user is a member.

Storing the user membership in an attribute of the group object. With this method, there is a group object that contains a list of the users who are members of the group. If your LDAP server uses this method, you need to specify the group to check under the LDAP mapping section of a User Group for which you want to match the user.

To determine the method to be used, Fortinet recommends checking the LDAP documentation for your server or using a third party LDAP browser e.g. from <http://directory.apache> to check the attributes of the server.

- Username—The user account that has permissions to search the LDAP server. This is needed so that FortiConnect can search for the user account and group mapping information.
- Password—The password for the user account that has permissions to search the LDAP server.

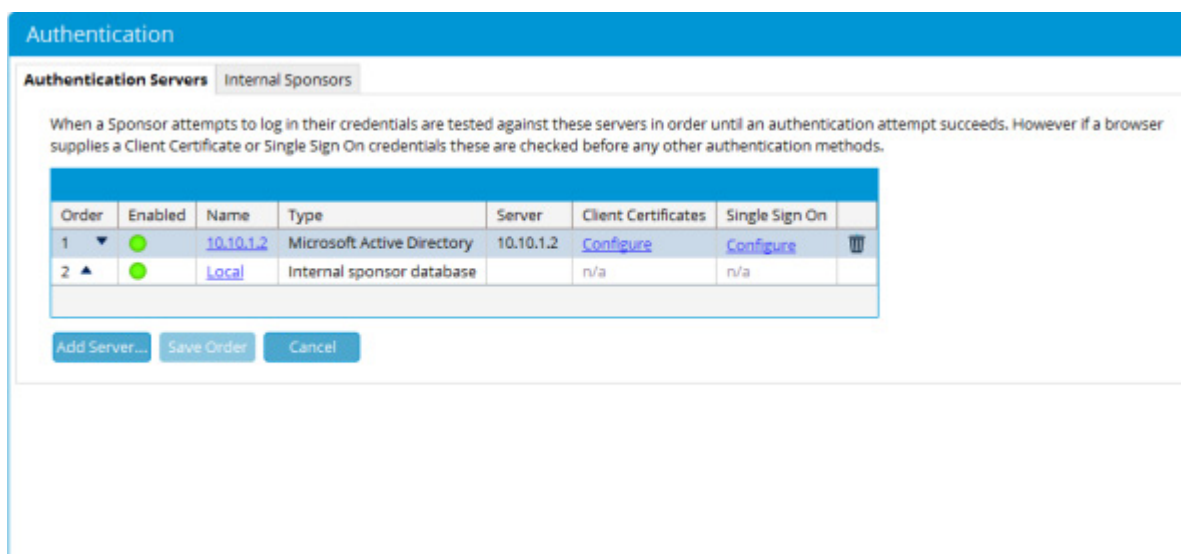
To provide resilience in the event of an LDAP server failure, you can enter multiple entries for high availability LDAP servers pointing to the same database. The Server name and URL need to be different in each entry.

FortiConnect attempts to authenticate sponsors against each LDAP server entry in the order specified by Authentication Order (as detailed in Configuring Sponsor Authentication Settings)

To verify that you have the correct LDAP credentials for connecting to your LDAP server,

Add an LDAP Server

1. From the administration interface, select Sponsor Portal > Authentication from the menu and click on the Authentication Servers tab as shown below.



2. Click the Add Server button.
3. In the Add LDAP Server page, from the drop down menu select the type of LDAP server you wish to add and enter all the details for authenticating against a specific LDAP server as shown in the screenshot below.

Add Authentication Server

Authentication Type: Generic LDAP

Server:

Hostname or IP Address

< Back Next > Exit

Note: When selecting Open LDAP the FortiConnect wizard will automatically populate and detect certain settings, For the purpose of the documentation, Generic LDAP will be used as an example as to detail all the settings FortiConnect requires.

4. Enter the following details as show below.

- **Name**—Type a text description of the LDAP Server Name or IP Address.
- **Server Type** - Server type is auto populated.
- **Server** - Server IP address is auto populated.
- **Encryption** - Select the Encryption method desired for this server. (If the certificate is not trusted then you will be given an option to upload a certificate. Click on **Choose File** to select one.)
- **Base DN**—This is the Distinguished Name of the container object from which an LDAP search to find the user is started, select the desired BASE DN from the drop down list such as OU=Users,O=merunetworks.com or OU=Engineering,O=merunetworks.

Add an LDAP Server

Add Authentication Server

Name: 10.10.1.2

Server Type: Generic LDAP

Server: 10.10.1.2

This server supports encryption, but you must use a hostname that matches the CN (Common Name) in the server's SSL certificate.

Encryption: None

Base DN: DC=identitynetworks,DC=com [server default]

< Back Next > Exit

5. Now click on next to continue and enter further LDAP settings.

Server

- Server - Enter Server IP Address
- Encryption - Enter Encryption method
- Non Default Port - Enter non default port number.
- Network Timeout - Enter the network timeout in seconds.
- BASE DN - This is the Distinguished Name of the container object from which an LDAP search to find the user is started, select the desired BASE DN from the drop down list such as OU=Users,O=merunetworks.com or OU=Engineering,O=merunetworks.
- Server Supports Paged Results - Click box to support this.
- Page Size - Enter page size if Server Supports Paged Results is checked.

Users

- Fixed Bind DN for login - Enter the Fixed Bind DN for login, if left blank the system will determine the Bind DN's automatically.
- User Name Query - Returns information for a user. Enter query here.

Groups

- Username Query Returns Groups - Check box to enable. Some LDAP server implementations (e.g. Active Directory or eDirectory) have the user's group memberships as an attribute of the

user. Other implementations (e.g. OpenLDAP) require an additional query be run to find a user's group memberships.

- User Group Membership Query - Returns the groups that a user is in when the query is run.
- Active Groups Query - Returns a list of groups when a query is run.

Attributes

- First Name - Enter the attribute that contains a user's First name.
- Last Name - Enter the attribute that contains a user's Last name.
- Email - Enter the attribute that contains a user's email address.
- Manager - Some LDAP Servers or user configurations may not have a manager attribute.
- Username - Enter the attribute that contains a user's username.
- Group name - Enter the attribute that contains a user's group name, if supported by the LDAP Server.
- UUID - UUDI of the Server

6. Click on next to continue

Add Authentication Server

The following settings are common defaults that may work on many LDAP servers, some detailed knowledge of your LDAP server may be required to modify and complete the configuration.

Server

Server: 10.10.1.2

Encryption: None

Port:

Network Timeout (seconds): 10

Base DN: DC=identitynetworks,DC=com

Server Supports Paged Results: ☒

Page Size: 1000

Users

Fixed Bind DN for Login:

If left blank the system will determine bind DN's automatically. %s in the value is replaced by the username.

Username Query: (uid=%s)

Returns information for a user. When the query is run %s is replaced with the username.

Email Query: (&(objectClass=Person)(mail=%s))

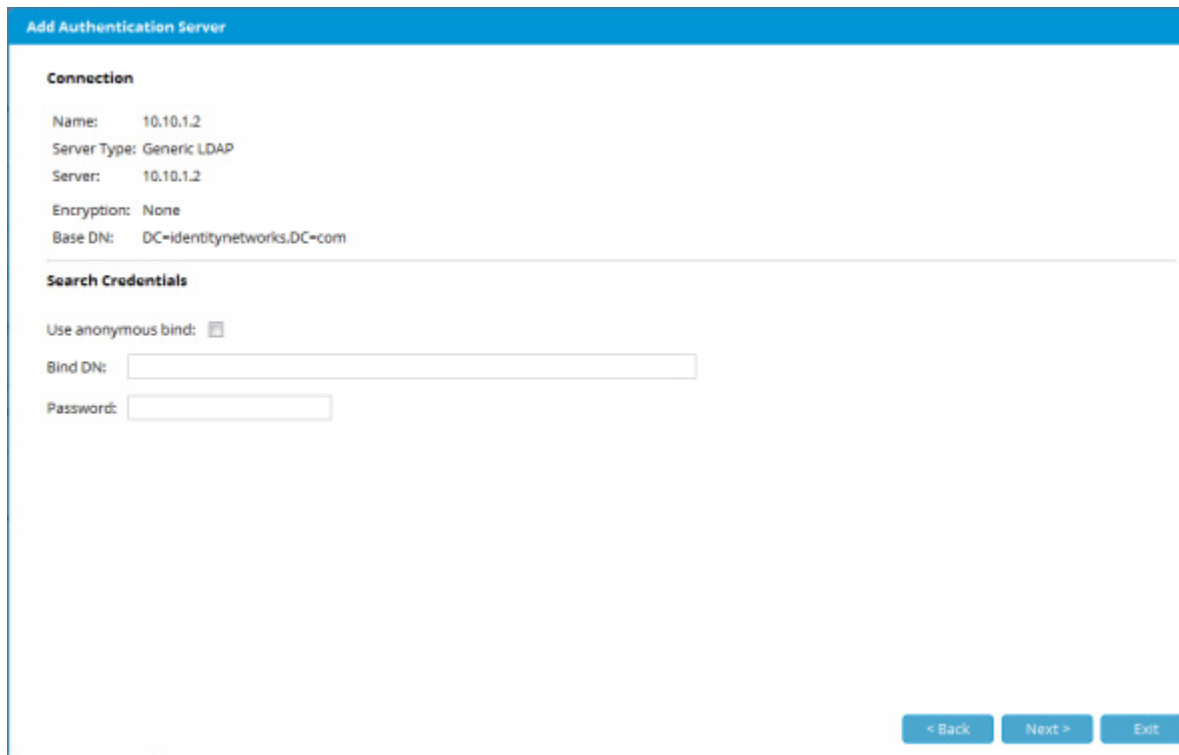
Returns information for a user. When the query is run %s is replaced with the e-mail address.

7. Now enter the Search Credentials as shown in the screenshot below.

- Use anonymous bind – Select the check box to enable.

Edit an Existing LDAP Server

- Password - The password for the user account that has permissions to search the LDAP server.
- Confirm —Repeat the password for confirmation.



The screenshot shows the 'Add Authentication Server' configuration page. It has a blue header bar with the title 'Add Authentication Server'. Below the header, there are two main sections: 'Connection' and 'Search Credentials'. The 'Connection' section contains the following fields: 'Name' (10.10.1.2), 'Server Type' (Generic LDAP), 'Server' (10.10.1.2), 'Encryption' (None), and 'Base DN' (DC=identitynetworks.DC=com). The 'Search Credentials' section contains a checkbox for 'Use anonymous bind' (unchecked), a text field for 'Bind DN', and a text field for 'Password'. At the bottom right of the form, there are three buttons: '< Back', 'Next >', and 'Exit'.

8. Click next to complete setup

Edit an Existing LDAP Server

1. From the administration interface, select Sponsor Portal > Authentication from the menu and click on the Authentication Servers tab as shown below.

Authentication

Authentication Servers Internal Sponsors

When a Sponsor attempts to log in their credentials are tested against these servers in order until an authentication attempt succeeds. However if a browser supplies a Client Certificate or Single Sign On credentials these are checked before any other authentication methods.

Order	Enabled	Name	Type	Server	Client Certificates	Single Sign On	
1 ▼	●	10.10.1.2	Generic LDAP	10.10.1.2	Configure	n/a	🗑️
2 ▲ ▼	●	10.10.1.2	Microsoft Active Directory	10.10.1.2	Configure	Configure	🗑️
3 ▲	●	Local	Internal sponsor database		n/a	n/a	

[Add Server...](#)
[Save Order](#)
[Cancel](#)

2. Click the underlined link of the LDAP Server you wish to edit.
3. In the Edit LDAP Server page, Edit the details as detailed below server as shown below.

Edit Authentication Server

Name:

Server Type: Generic LDAP

Server: 10.10.1.2

This server supports encryption, but you must use a hostname that matches the CN (Common Name) in the server's SSL certificate.

Encryption:

Base DN:

[< Back](#)
[Next >](#)
[Exit](#)

- Name—Type a text description of the LDAP Server Name or IP Address.
- Server Type - Server type is auto populated.

Edit an Existing LDAP Server

- **Server** - Server IP address is auto populated.
 - **Encryption** - Select the Encryption method desired for this server. (If the certificate is not trusted then you will be given an option to upload a certificate. Click on Choose File to select one.)
 - **Base DN**—This is the Distinguished Name of the container object from which an LDAP search to find the user is started, select the desired BASE DN from the drop down list such as OU=Users,O=merunetworks.com or OU=Engineering,O=merunetworks.
4. Now click on next to continue and edit further LDAP settings as shown in the screenshot below.

Edit Authentication Server

Server

Server: 10.10.1.2

Encryption: None

Port:

Network Timeout (seconds): 10

Base DN: DC=identitynetworks.DC=com

Server Supports Paged Results: ☒

Page Size: 1000

Users

Fixed Bind DN for Login:

If left blank the system will determine bind DN's automatically. %s in the value is replaced by the username.

Username Query: uid=%s

Returns information for a user. When the query is run %s is replaced with the username.

Email Query: (&(objectClass=Person)(mail=%s))

Returns information for a user. When the query is run %s is replaced with the e-mail address.

Groups

Some LDAP server implementations (e.g. Active Directory or eDirectory) have the user's group memberships as an attribute of the user. Other implementations

Server

- **Server** - Enter Server IP Address
- **Encryption** - Enter Encryption method
- **Non Default Port** - Enter non default port number.
- **Network Timeout** - Enter the network timeout in seconds.
- **BASE DN** - This is the Distinguished Name of the container object from which an LDAP search to find the user is started, select the desired BASE DN from the drop down list such as OU=Users,O=merunetworks.com or OU=Engineering,O=merunetworks.

- Server Supports Paged Results - Click box to support this.
- Page Size - Enter page size if Server Supports Paged Results is checked.

Users

- Fixed Bind DN for login - Enter the Fixed Bind DN for login, if left blank the system will determine the Bind DN's automatically.
- User Name Query - Returns information for a user. Enter query here.

Groups

- Username Query Returns Groups - Check box to enable. Some LDAP server implementations (e.g. Active Directory or eDirectory) have the user's group memberships as an attribute of the user. Other implementations (e.g. OpenLDAP) require an additional query be run to find a user's group memberships.
- User Group Membership Query - Returns the groups that a user is in when the query is run.
- Active Groups Query - Returns a list of groups when a query is run.

Attributes

- First Name - Enter the attribute that contains a user's First name.
- Last Name - Enter the attribute that contains a user's Last name.
- Email - Enter the attribute that contains a user's email address.
- Username - Enter the attribute that contains a user's username.
- Group name - Enter the attribute that contains a user's groups, if supported by the LDAP Server.

5. Click on next to continue

6. Now enter the Search Credentials as shown below.

- Use anonymous bind – Select the check box to enable.
- Password - The password for the user account that has permissions to search the LDAP server.
- Confirm –Repeat the password for confirmation.

Delete an Existing LDAP Server Entry

Edit Authentication Server

Connection

Name: 10.10.1.2
Server Type: Generic LDAP
Server: 10.10.1.2
Encryption: None
Base DN: DC=identitynetworks.DC=com

Search Credentials

Use anonymous bind: ☐

Bind DN:

Password:

< Back Next > Exit

7. Click next to complete setup

Delete an Existing LDAP Server Entry

1. From the administration interface, select Sponsor Portal > Authentication from the menu and click on the Authentication Servers tab.
2. Select the LDAP Server from the list as shown below.

Authentication

Authentication Servers | Internal Sponsors

When a Sponsor attempts to log in their credentials are tested against these servers in order until an authentication attempt succeeds. However if a browser supplies a Client Certificate or Single Sign On credentials these are checked before any other authentication methods.

Order	Enabled	Name	Type	Server	Client Certificates	Single Sign On	
1 ▼	●	10.10.1.2	Generic LDAP	10.10.1.2	Configure	n/a	🗑️
2 ▲	●	10.10.1.2	Microsoft Active Directory	10.10.1.2	Configure	Configure	🗑️
3 ▲	●	Local	Internal sponsor database		n/a	n/a	

[Add Server...](#) [Save Order](#) [Cancel](#)

3. Choose the server you wish to delete by clicking the bin icon to the right of the Status field.
4. Confirm deletion of the LDAP Server at the prompt.

If there are any errors, the LDAP Server is not changed and an error message is displayed at the top of the page. If successfully deleted, a success message is displayed at the top of the page and you can perform additional LDAP Server operations.

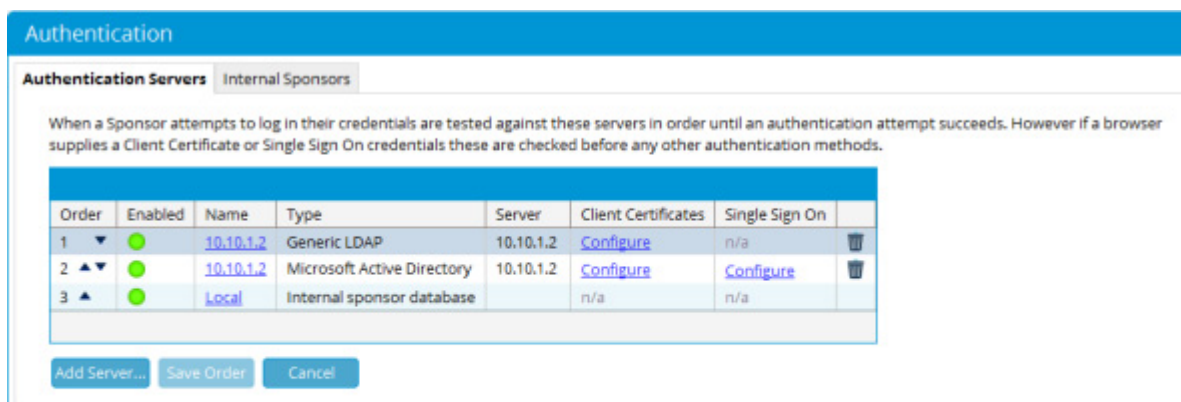
Configuring Novell eDirectory Server Authentication

The following section describes how to Configure Novell eDirectory Server Authentication.

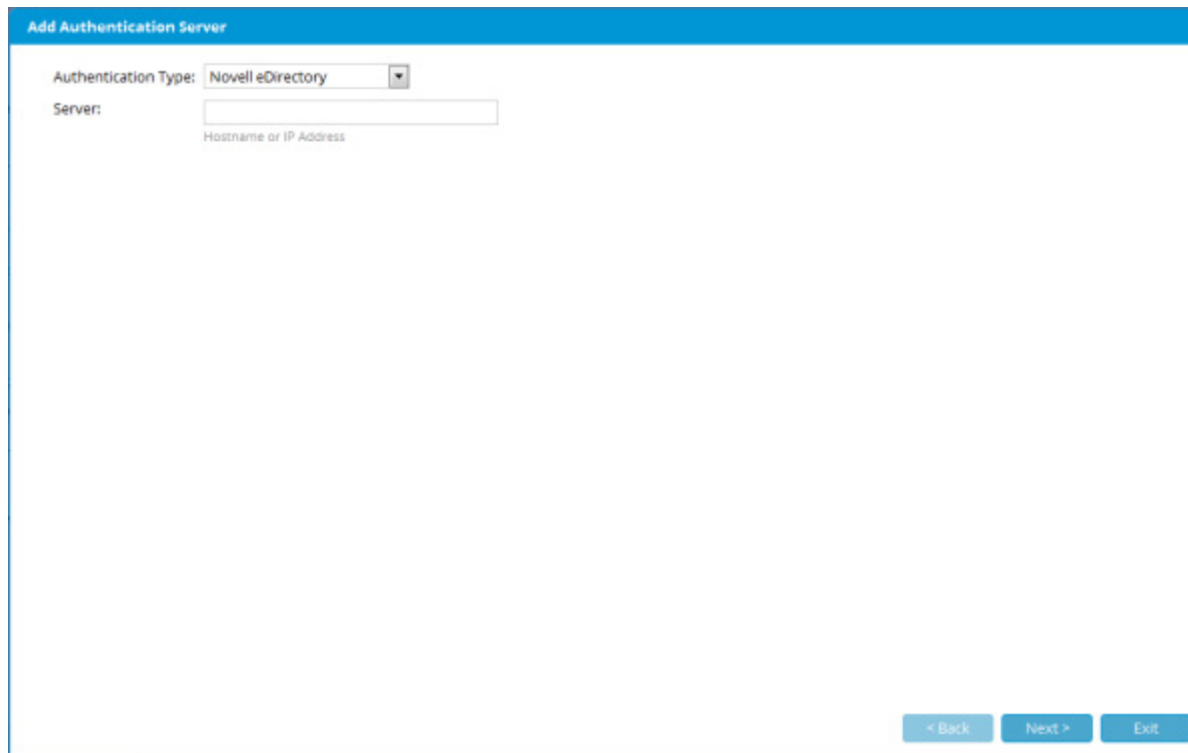
- Add a Novell eDirectory Server.
- Edit a Novell eDirectory Server.
- Delete a Novell eDirectory Server.

Add a Novell eDirectory Server

1. From the administration interface, select Sponsor Portal > Authentication from the menu and click on the Authentication Servers tab as shown below.



2. Click the Add Server button.
3. In the Add Authentication Server page, from the drop down menu select Novell eDirectory and enter the hostname or the IP address of the Novell eDirectory Server you wish to authenticate against.



Add Authentication Server

Authentication Type: Novell eDirectory ▼

Server:

Hostname or IP Address

< Back Next > Exit

4. Enter the following details as show below.

- Name—Type a text description of the Novell eDirectory Server Server Name or IP Address.
- Server Type - Server type is auto populated.
- Server - Server IP address is auto populated.
- Encryption - Select the Encryption method desired for this server. (If the certificate is not trusted then you will be given the option to upload a certificate. Click on Choose file to select)
- Base DN—This is the Distinguished Name of the container object from which a Novell eDirectory Server search to find the user is started, select the desired BASE DN from the drop down list such as OU=Users,O=merunetworks.com or OU=Engineering,O=merunetworks.

Add a Novell eDirectory Server

The screenshot shows a configuration window titled "Add Authentication Server". It contains the following fields and options:

- Name:** 10.10.1.2
- Server Type:** Novell eDirectory
- Server:** 10.10.1.2
- Encryption:** None (dropdown menu)
- Certificate:** Choose File (button) | No file chosen (text)
- Base DN:** DC=identitynetworks.DC=com [server default] (dropdown menu)

Below the fields, there is a message: "This server supports encryption, but its certificate cannot be validated. You must upload its certificate or its root certificate to continue:". At the bottom right, there are three buttons: "< Back", "Next >", and "Exit".

5. Now enter the Search Credentials as shown in the screenshot below.
- Use anonymous bind – Select the check box to enable.
 - Password - The password for the user account that has permissions to search the Novell eDirectory server.
 - Confirm –Repeat the password for confirmation.

Add Authentication Server

Connection

Name: 10.10.1.2
Server Type: Novell eDirectory
Server: 10.10.1.2
Encryption: None
Base DN: DC=identitynetworks.DC=com

Search Credentials

Use anonymous bind: ☐

Bind DN:

Password:

< Back Next > Exit

6. Click Next to complete the setup.

Edit a Novell eDirectory Server

1. From the administration interface, select Sponsor Portal > Authentication from the menu and click on the Authentication Servers tab as shown below.

Edit a Novell eDirectory Server

Authentication

Authentication Servers Internal Sponsors

When a Sponsor attempts to log in their credentials are tested against these servers in order until an authentication attempt succeeds. However if a browser supplies a Client Certificate or Single Sign On credentials these are checked before any other authentication methods.

Order	Enabled	Name	Type	Server	Client Certificates	Single Sign On	
1 ▼	●	<u>10.10.1.2</u>	Novell eDirectory	10.10.1.2	Configure	n/a	🗑
2 ▲▼	●	<u>10.10.1.2</u>	Generic LDAP	10.10.1.2	Configure	n/a	🗑
3 ▲▼	●	<u>10.10.1.2</u>	Microsoft Active Directory	10.10.1.2	Configure	Configure	🗑
4 ▲	●	<u>Local</u>	Internal sponsor database		n/a	n/a	

[Add Server...](#) [Save Order](#) [Cancel](#)

- Click the underlined link of the Novell eDirectory Server you wish to edit.
- In the Edit Authentication Server page, Edit the details as detailed below server as shown below.

Edit Authentication Server

Name:

Server Type: Novell eDirectory

Server:

Encryption:

This server supports encryption, but its certificate cannot be validated. You must upload its certificate or its root certificate to continue:

Certificate: No file chosen

Base DN:

[< Back](#) [Next >](#) [Exit](#)

- Name—Type a text description of the Novell eDirectory Server Name or IP Address.
- Server Type - Server type is auto populated.

- **Server** - Server IP address is auto populated.
 - **Encryption** - Select the Encryption method desired for this server. (If the certificate is not trusted then you will be given an option to upload a certificate. Click on Choose File to select one.)
 - **Base DN**—This is the Distinguished Name of the container object from which a Novell eDirectory Server search to find the user is started, select the desired BASE DN from the drop down list such as OU=Users,O=merunetworks.com or OU=Engineering,O=merunetworks.
4. Now click on next to continue and edit further Novell eDirectory Server settings as shown in the screenshot below.

Edit Authentication Server

Connection

Name: 10.10.1.2
 Server Type: Novell eDirectory
 Server: 10.10.1.2
 Encryption: None
 Base DN: DC=identitynetworks,DC=com

Search Credentials

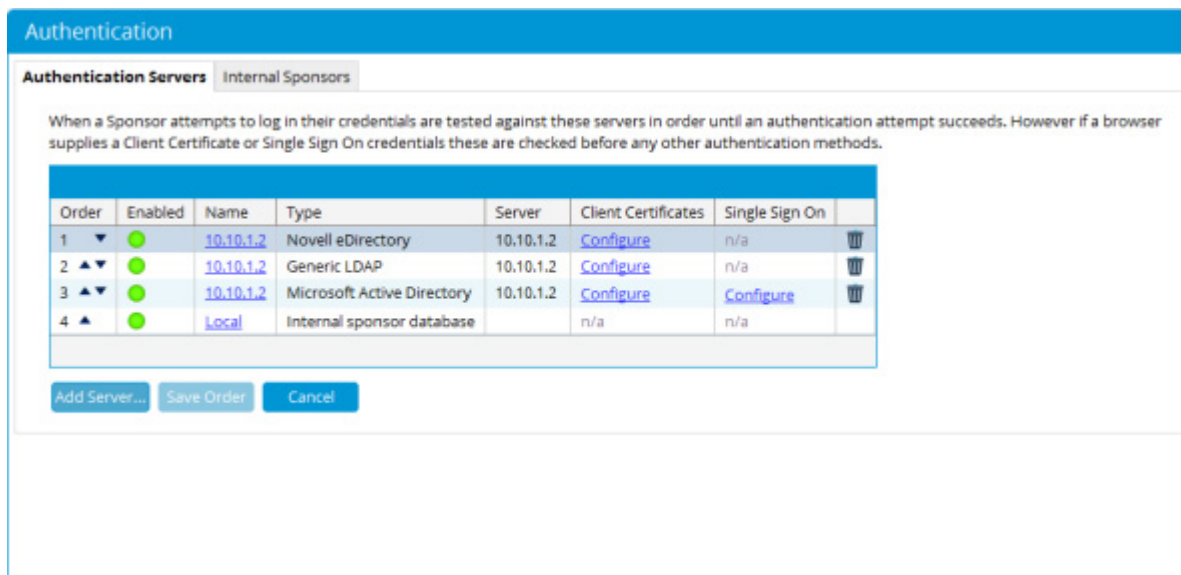
Use anonymous bind: ☐
 Bind DN:
 Password:

< Back Next > Exit

- **Use anonymous bind** – Select the check box to enable.
 - **Password** - The password for the user account that has permissions to search the Novell eDirectory Server.
 - **Confirm** –Repeat the password for confirmation.
5. Click on Next to complete.

Delete a Novell eDirectory Server

1. From the administration interface, select Sponsor Portal > Authentication from the menu and click on the Authentication Servers tab.
2. Select the Novell eDirectory Server from the list as shown below.



3. Choose the server you wish to delete by clicking the bin icon to the right of the Status field.
4. Confirm deletion of the Novell eDirectory Server at the prompt.

Configuring RADIUS Authentication

RADIUS authentication allows FortiConnect to authenticate sponsors using their existing RADIUS user accounts. The sponsors need not have another set of user names and passwords to authenticate to FortiConnect. It also enables the administrator to quickly roll out User Access because there is no need to create and manage additional local sponsor accounts. RADIUS authentication allows you to do the following:

- Add a RADIUS Server
- Edit an Existing RADIUS Server
- Delete an Existing RADIUS Server Entry

Add a RADIUS Server

1. From the administration interface, select Sponsor Portal > Authentication. Select the Authentication Servers tab as shown below.

Authentication

Authentication Servers Internal Sponsors

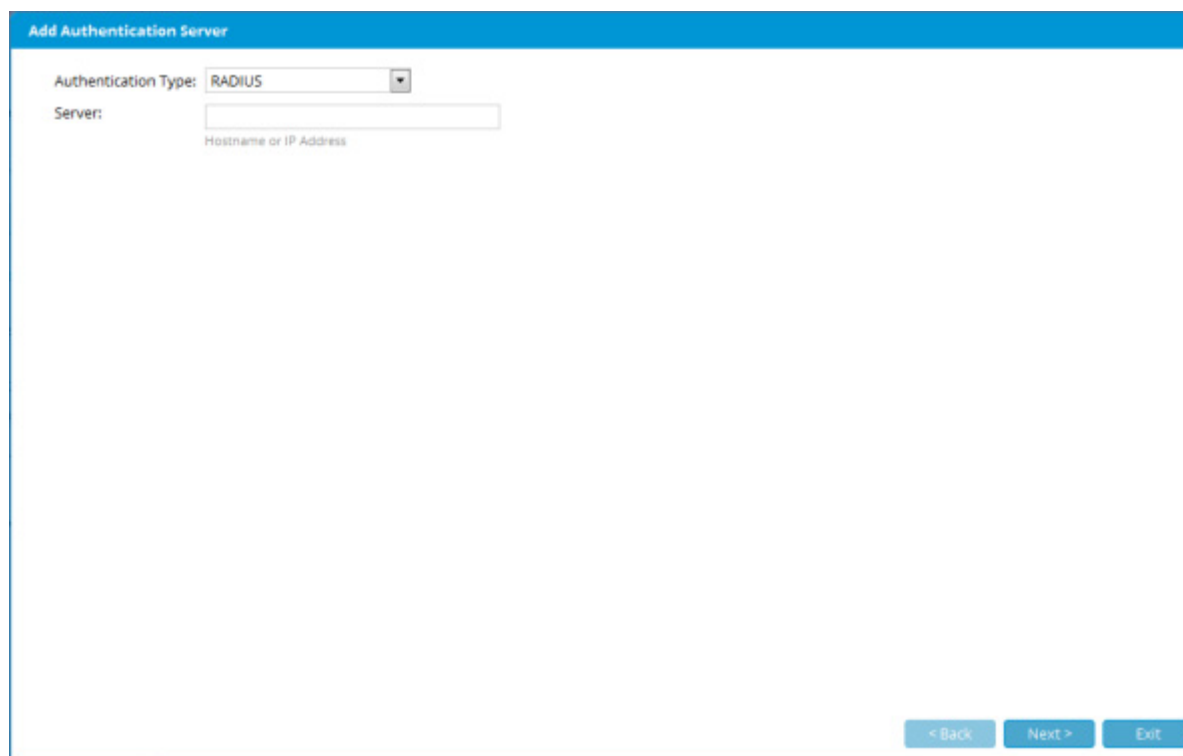
When a Sponsor attempts to log in their credentials are tested against these servers in order until an authentication attempt succeeds. However if a browser supplies a Client Certificate or Single Sign On credentials these are checked before any other authentication methods.

Order	Enabled	Name	Type	Server	Client Certificates	Single Sign On	
1 ▼	●	10.10.1.2	Novell eDirectory	10.10.1.2	Configure	n/a	🗑️
2 ▲▼	●	10.10.1.2	Generic LDAP	10.10.1.2	Configure	n/a	🗑️
3 ▲▼	●	10.10.1.2	Microsoft Active Directory	10.10.1.2	Configure	Configure	🗑️
4 ▲	●	Local	Internal sponsor database		n/a	n/a	

[Add Server...](#) [Save Order](#) [Cancel](#)

2. Click the Add Server button
3. From the Authentication type drop down menu, select Radius.
4. In the Server text box insert the Hostname or IP address of the RADIUS server as shown below, and click Next

Add a RADIUS Server



Add Authentication Server

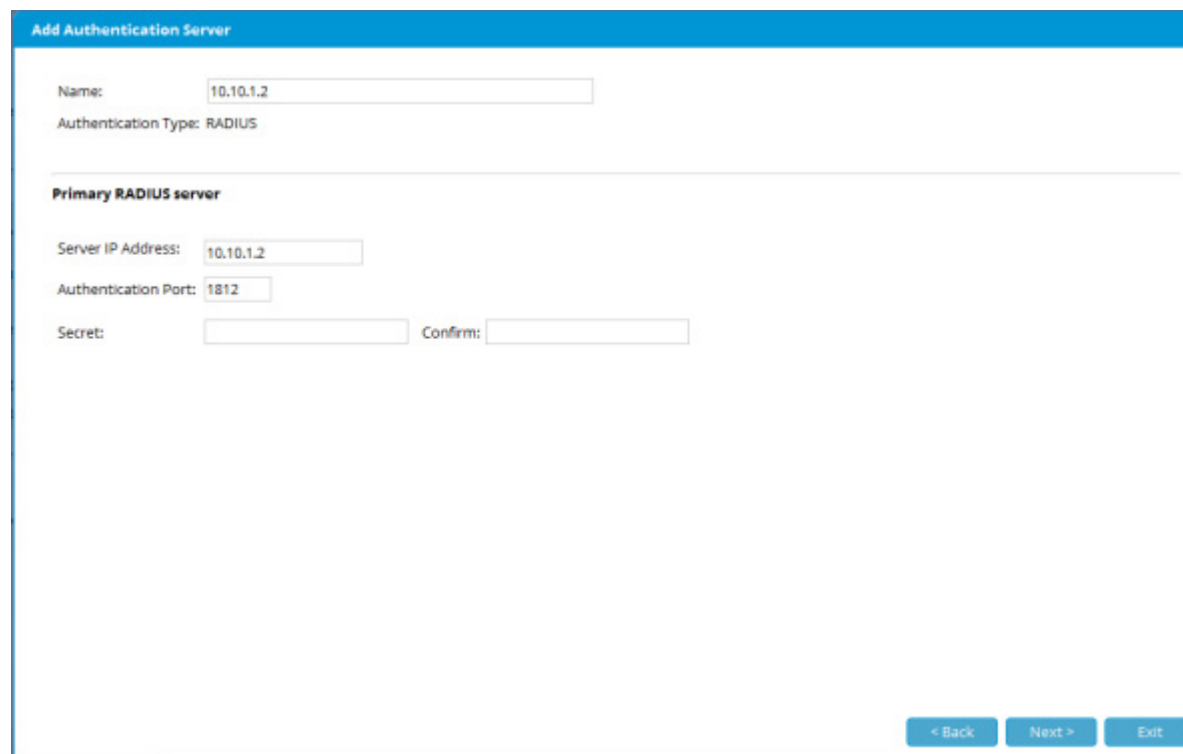
Authentication Type: RADIUS

Server:

Hostname or IP Address

< Back Next > Exit

5. Insert the requested Radius Server details into the appropriate fields as shown in the screenshot below.



Add Authentication Server

Name:

Authentication Type: RADIUS

Primary RADIUS server

Server IP Address:

Authentication Port:

Secret: Confirm:

< Back Next > Exit

- **Server Name**—Type a text description of the RADIUS Server Name. For example: Fortinet RADIUS - radius.identitynetworks.com.
- **Server**—Enter the IP address or domain name of the RADIUS server.
- **Port**—Enter the UDP port used to connect to the RADIUS server. The common ports for RADIUS authentication are ports 1645 or 1812.
- **RADIUS Secret**—The shared secret used to secure the communications between FortiConnect and the RADIUS server.
- **Confirm**—Repeat the shared secret for confirmation.

6. Click the Next button to complete.

Add Fortigate as a RADIUS server

Fortigate can be added as a Radius client in FortiConnect. However, there are following limitations:

- COA is not supported. Due to this, Sponsor disable and disconnect feature will not work.
- Device Authentication feature will not work as Fortigate does not send NAS IP Address/Called-Station-Id parameters.
- OAuth feature is not supported
- As Fortigate does not send AP name and AP id some guest reports and accounting logs will have empty fields against them.
- Redirection URL after successful guest authentication **must** be set in Fortigate configuration.
- In Mac / iPad, when using Safari to perform guest authentication, intermittently the browser will timeout or will take long time to redirect to the portal success page.

To integrate, start by creating a RADIUS client entry of type Fortigate. Provide Fortigate server IP address.

The screenshot displays the 'RADIUS Clients' configuration interface. On the left is a navigation menu with options: HOME, NETWORK ACCESS POLICY, POLICY SETTINGS, SPONSOR PORTAL, GUEST PORTALS, SMART CONNECT, and DEVICES. Under 'DEVICES', 'RADIUS Clients' is selected. The main panel shows the 'RADIUS Clients' form with tabs for Client, Attributes, SNMP, MAC Authentication, and RadSec Authentication. The 'Client' tab is active. Fields include: Name (Fortigate), Device IP Address / Prefix Length (172.18.26.26/32), Secret (empty), Confirm (empty), Type (Fortigate), and Description (empty). A note below the Type dropdown states: 'If your RADIUS client vendor is not listed please select Generic RADIUS Device'. At the bottom are 'Save' and 'Cancel' buttons.

Add a RADIUS Server

In the attributes tab, add Acct-Interim-Interval = <nnn> (between 600 - 86400 seconds) entry

The screenshot shows the 'RADIUS Clients' configuration page in the FortiGate WebUI. The 'Attributes' tab is active. A new attribute is being added with the following details:

- Vendor: IETF
- Attribute: Access-Loop-Encapsulation
- Value: Acct-Interim-Interval = 600

The attribute is listed in a table with buttons to Move up, Remove, or Move down. Save and Cancel buttons are at the bottom.

After you have completed configuring Fortigate server details in the FortiConnect server, log in to your Fortigate server and do the following to complete the integration.

Step 1 In the Fortigate server WebUI, go to WiFi Controller > SSID. Create a new SSID and ensure that you provide details as listed after the following screenshot.

The screenshot shows the 'WiFi Settings' page in the FortiGate WebUI. The SSID is 'fortinet-clear'. The configuration details are as follows:

- SSID: fortinet-clear
- Security Mode: Captive Portal
- Portal Type: Authentication
- Authentication Portal: External 172.19.40.249/portal/172.18.26.26
- User Groups: Guest-group
- Redirect after Captive Portal: Specific URL http://172.19.40.249/portal/login/172.18.26.26/success
- Broadcast SSID: ☒
- Block Intra-SSID Traffic: ☒
- Maximum Clients: ☐
- Optional VLAN ID: 0

1. Set Security Mode to *Captive Portal*.

2. Select Portal Type as *Authentication*.

3. Enter the Authentication Portal address in this format: <meruConnect-serverIP>/portal/Fortigate-serverIP>.

For example, if FortiConnect server IP is 172.19.40.249 and Fortigate server IP is 172.18.26.26, then your IP address is 172.19.40.249/portal/172.18.26.26.

4. Provide a destination URL to Redirect after Captive Portal authentication.

Step 2 Go to Wifi Controller > FortiAP Profiles and create or edit a profile. In the profile, set the SSID of each radio to the SSID created in step 1.

The screenshot shows the FortiAP Profile configuration page. On the left, there is a sidebar with a tree view containing 'Radio 1' and 'Radio 2'. The main area displays configuration options for the selected radio. For both Radio 1 and Radio 2, the 'SSID' field is highlighted with a red box and a red arrow. A 'Please Select' dropdown menu is open for each SSID field, showing the option 'forti-clear (SSID: fortinet-clear)'. Other visible settings include 'Select Channel Width' (20MHz), 'Channel' (36, 40, 44, 48, 149, 153, 157, 161, 165), 'Auto TX Power Control' (Disable), 'TX Power' (100%), 'Mode', 'Spectrum Analysis', 'WIDS Profile' (Click to set...), 'Radio Resource Provision', 'Client Load Balancing' (Frequency Handoff, AP Handoff), 'Band' (2.4GHz 802.11n/g/b), and 'Channel' (1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11).

Step 3 Go to Policies and Objects > Objects > Addresses. Create a new entry with a name for the FortiConnect Server and its IP address.

The screenshot shows the 'Addresses' configuration page in FortiConnect. The 'Name' field is set to 'Meru Connect RADIUS'. The 'Type' is set to 'IP/Netmask'. The 'Subnet / IP Range' is set to '172.18.26.26/255.255.255.255'. The 'Interface' is set to 'any'. The 'Show in Address List' checkbox is checked. The 'Comments' field is empty. The 'OK' and 'Cancel' buttons are at the bottom right.

Add a RADIUS Server

Step 4 Go to Policies and Objects > Policy > IPv4. Create the following rules:

Seq.#	From	To	Source	Destination	Schedule	Service	Action	NAT	SSL Inspection	Log	Count
1	any	forti-clear (SSID: fortinet-clear)	Meru Connect	all	always	ALL	ACCEPT	Enable		All	0 Packets / 0 B
2	forti-clear (SSID: fortinet-clear)	any	all	Meru Connect	always	ALL	ACCEPT	Enable		All	96,893 Packets / 57.75 MB
3	any	any	all	all	always	DNS DHCP	ACCEPT	Enable		All	62,194 Packets / 6.37 MB
4	forti-clear (SSID: fortinet-clear)	any	all Guest-group	all	always	ALL	ACCEPT	Enable		UTM	2,053 Packets / 1.15 MB

Step 5 Go to User & Device > Authentication > RADIUS Servers. Create a new entry of the FortiConnect server. The secret key entered here should be used while adding the Fortigate server in FortiConnect. Ensure that you enter the Fortigate server IP address as the *NAS IP / Called Station ID*.

Name	Meru Connect RADIUS	
Primary Server IP/Name	172.19.40.249	
Primary Server Secret	••••••••	Test Connectivity
Secondary Server IP/Name		
Secondary Server Secret		Test Connectivity
Authentication Method	<input checked="" type="radio"/> Default <input type="radio"/> Specify	
NAS IP / Called Station ID	172.18.26.26	This Fortigate Server IP
Include in every User Group	<input checked="" type="checkbox"/>	
<div>OK</div> <div>Cancel</div>		

Step 6 Now, go to the Fortigate CLI, and execute the following commands to complete the integration:

Allow external web access

```
# set captive portal exempt enable
```

Configure accounting time interval

```
# set acct-interim-interval [duration] (between 600 - 86400 seconds)
```

Configure FortiConnect as the Radius accounting server

```
# config accounting-server
```

```
# edit 1
```

```
# set status enable
```

```
# set server <IP Address of FortiConnect>
```

```
# Set secret <Secret>
```

Edit an Existing RADIUS Server

1. From the administration interface, select Sponsor Portal > Authentication and select the Authentication Servers tab.
2. Select the RADIUS server from the list and click the underlined name of the server you wish to edit as shown below.

Authentication

Authentication Servers Internal Sponsors

When a Sponsor attempts to log in their credentials are tested against these servers in order until an authentication attempt succeeds. However if a browser supplies a Client Certificate or Single Sign On credentials these are checked before any other authentication methods.

Order	Enabled	Name	Type	Server	Client Certificates	Single Sign On	
1 ▼	●	<u>10.10.1.2</u>	RADIUS	10.10.1.2	n/a	n/a	🗑️
2 ▲▼	●	10.10.1.2	Novell eDirectory	10.10.1.2	Configure	n/a	🗑️
3 ▲▼	●	10.10.1.2	Generic LDAP	10.10.1.2	Configure	n/a	🗑️
4 ▲▼	●	10.10.1.2	Microsoft Active Directory	10.10.1.2	Configure	Configure	🗑️
5 ▲	●	Local	Internal sponsor database		n/a	n/a	

[Add Server...](#) [Save Order](#) [Cancel](#)

3. In the Edit RADIUS Server Details page as shown below, edit the details for authenticating against this RADIUS server.

Edit an Existing RADIUS Server

Edit Authentication Server

Name:

Authentication Type: RADIUS

Primary RADIUS server

Server IP Address:

Authentication Port:

Secret: Confirm:

< Back Next > Exit

4. Modify settings as needed:

- **Server IP Address**—Enter the IP address or domain name of the RADIUS server.
- **Port**—Enter the UDP port used to connect to the RADIUS server. The common ports for RADIUS authentication are ports 1645 or 1812.
- **RADIUS Secret**—The shared secret used to secure the communications between FortiConnect and the RADIUS server.

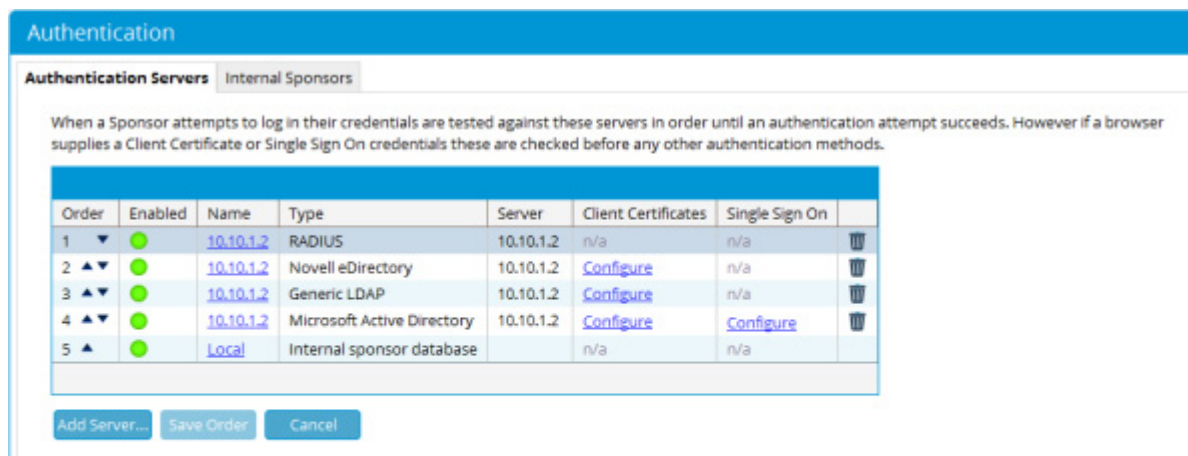
Note: If you do not want to change the shared secret, leave the Secret and Confirm fields to retain the existing shared secret.

- **Enabled**—Check the checkbox to enable FortiConnect to use this RADIUS server to authenticate sponsors. If not checked, the RADIUS server will not be used.

5. Click the Next button.

Delete an Existing RADIUS Server Entry

1. From the administration interface, select Sponsor Portal > Authentication and select the Authentication Servers tab.
2. Find the RADIUS server in the list that you wish to delete and click the bin icon to the right of the Status field as shown below.



3. Confirm deletion of the RADIUS server at the prompt.

If there are any errors, the RADIUS server is not changed and an error message is displayed at the top of the page. If successfully deleted, a success message is displayed at the top of the page and you can perform additional RADIUS operations.

Active Directory Single Sign-On

The Active Directory Single Sign-On (AD SSO) feature uses Kerberos between the client's web browser and FortiConnect to automatically authenticate a Sponsor against an Active Directory Domain Controller.

An Active Directory Domain Controller in the same domain as the single sign on configuration must have been previously configured as described in Configuring Active Directory (AD) Authentication.

Requirements for Active Directory Single Sign-On

The following requirements must be met for Active Directory Single Sign-On to be configured successfully:

- DNS must be configured and working on FortiConnect
- DNS must be configured and working on the Domain Controller
- Both of the following DNS entries for FortiConnect must be defined and must be available to both FortiConnect and all Windows servers in the domain:
 - i. Forward (“A”) record
 - ii. Reverse (“PTR”) record
- Both of the following DNS entries for the Domain Controller must be defined and must be available to both FortiConnect and all Windows servers in the domain:
 - i. Forward (“A”) record
 - ii. Reverse (“PTR”) record
- FortiConnect time settings must be synchronized with the Active Directory Domain
- Sponsors web browser may require configuration to allow the single sign on function
- Single Sign on must be configured separately for each replicated server

If any of these settings are not met, then AD SSO configuration will fail.

Note: Fortinet strongly recommends configuring NTP so that time is synchronized with the Active Directory Domain. Single Sign-On will fail if the time on the FortiConnect appliance differs by more than 5 minutes from the client or the domain.

Configuring Active Directory Single Sign-On

1. Configure an Active Directory Server as described in [Configuring Active Directory \(AD\) Authentication](#). An Active Directory Server is needed so that users performing Single Sign-On can be correctly mapped against a sponsor group. The Active Directory Server must be in the same domain as in the Single Sign-On settings that you undertake.
2. From the administration interface, select **Sponsor Portal > Authentication** from the left menu and click on **Configure** under the **Single Sign On** column for the domain that you want to enable AD Single Sign On, as shown below.

Authentication Servers Internal Sponsors

When a Sponsor attempts to log in their credentials are tested against these servers in order until an authentication attempt succeeds. However if a browser supplies a Client Certificate or Single Sign On credentials these are checked before any other authentication methods.

Order	Enabled	Name	Type	Server	Client Certificates	Single Sign On	
1 ▼	●	10.10.1.2	RADIUS	10.10.1.2	n/a	n/a	🗑️
2 ▲▼	●	10.10.1.2	Novell eDirectory	10.10.1.2	Configure	n/a	🗑️
3 ▲▼	●	10.10.1.2	Generic LDAP	10.10.1.2	Configure	n/a	🗑️
4 ▲▼	●	10.10.1.2	Microsoft Active Directory	10.10.1.2	Configure	Configure	🗑️
5 ▲	●	Local	Internal sponsor database		n/a	n/a	

[Add Server...](#)
[Save Order](#)
[Cancel](#)

3. Enter the Domain Admin Username and Password in the fields provided.

4. Click on Next then click on Close to finish.

Sponsors you have created on Active Directory should now be able to login to the domain and access the Sponsor user interface. Sponsors should be entering the Domain name in the browser and not the IP Address of FortiConnect.

Note: If you have multiple FortiConnect appliances you will need to configure single sign on each appliance. This is so the account for each FortiConnect is successfully created in Active Directory.

Client Certificates

If your infrastructure is set up to use Client Certificates you may configure FortiConnect to accept a sponsor's Client Certificate as an alternative to logging in with a username and password.

The Client Certificate is installed on each sponsor's browser and typically the management of these certificates is managed by your local administrators.

- The following chapter details how to install and use your client certificates with FortiConnect.

Note: Client Certificate Authentication is not supported with RADIUS and local sponsor authentication.

Installing Client Certificates

In order to configure Client Certificate support you must possess a sample Client Certificate (possibly your own) that is in PKCS#12, PEM or DER format. FortiConnect will inspect this certificate and attempt to find a user in the selected authentication server based upon the certificate contents.

To use client certificates with FortiConnect follow the instructions below.

1. From the FortiConnect administration interface select Sponsor Portal --> Authentication.

Authentication Servers

Internal Sponsors

When a Sponsor attempts to log in their credentials are tested against these servers in order until an authentication attempt succeeds. However if a browser supplies a Client Certificate or Single Sign On credentials these are checked before any other authentication methods.

Order	Enabled	Name	Type	Server	Client Certificates	Single Sign On	
1	●	10.10.1.2	RADIUS	10.10.1.2	n/a	n/a	🗑
2	●	10.10.1.2	Novell eDirectory	10.10.1.2	Configure	n/a	🗑
3	●	10.10.1.2	Generic LDAP	10.10.1.2	Configure	n/a	🗑
4	●	10.10.1.2	Microsoft Active Directory	10.10.1.2	Configure	Configure	🗑
5	●	Local	Internal sponsor database		n/a	n/a	

Add Server...

Save Order

Cancel

2. Click on the Configure link underneath the Client Certificates column.

Configure Client Certificates

To configure client certificates you can upload a sample user certificate. By inspecting this certificate the system will automatically determine how to map the client certificate to a user on an authentication server.

☒ Parse a sample PKCS#12 file

PKCS#12 File: No file chosen
Files usually end in a p12 or pkcs12 extension

Password:
The password is only used to extract the certificate from the PKCS#12 file. It is not stored.

☐ Parse a sample X.509 certificate in PEM or DER format


Certificate: No file chosen
Files usually end in a pem, cer, der or crt extension

3. Depending on your certificates file type, select the appropriate parsing method and then click on the browse button to browse to and select your certificate file. If PKCS#12 has been selected as your format you must also enter the Password of the file and then click on next.

Installing Client Certificates

Sample Client Certificate
Common Name (CN): John Carter
Subject DN: /C=GB/ST=Berkshire/L=Newbury/O=My Company Ltd/CN=John Carter/emailAddress=johncarter@merutest.com
Parsed Subject DN: CN=John Carter,O=My Company Ltd,L=Newbury,ST=Berkshire,C=GB
Email Address: johncarter@merutest.com
User ID: <Not part of certificate>
User Principal Name: <Not part of certificate>

Find user on server by mapping Client Certificate to user attribute .
[Advanced >](#)

User Search Results
 No user found

- FortiConnect will attempt to find a user on your authentication server using the certificate properties. If an initial search finds no matching results, you will be required to change your server mapping accordingly using the drop down menus to obtain the results as shown in the example below.

Note: The advanced setting lets you perform regular expression replacements on certificate properties before searching in your authentication server.

Sample Client Certificate

Common Name (CN): John Carter
 Subject DN: /C=GB/ST=Berkshire/L=Newbury/O=My Company Ltd/CN=John Carter/emailAddress=johncarter@merutest.com
 Parsed Subject DN: CN=John Carter,O=My Company Ltd,L=Newbury,ST=Berkshire,C=GB
 Email Address: johncarter@merutest.com
 User ID: <Not part of certificate>
 User Principal Name: <Not part of certificate>

Find user on server by mapping Client Certificate to user attribute .
[Advanced »](#)

User Search Results

☒ User found

CN: John Carter
 DN: CN=John Carter,CN=Users,DC=merutest,DC=com
 Email Address: <Not set>
 Username: johncarter
 User Principal Name: johncarter@merutest.com

5. Some authentication servers have a copy of the full client certificate of a user as part of the user properties. As an additional check FortiConnect can directly compare that Client Certificate with the one supplied by the browser. The SSL renegotiation option allows FortiConnect to support the old and insecure method of authenticating with Client Certificates. If your browsers have been updated you may deselect this option.

Certificate Matching

Some authentication servers have the client certificate of each user. We can compare that certificate with the one supplied by the browser and the user will only be logged in if the certificates match.

This authentication server does not appear to store the user's certificate.

☐ Verify the user's certificate stored on the server matches the client certificate supplied by the browser.

SSL Renegotiation

In October 2009 a serious SSL vulnerability ([CVE-2009-3555](#)) was disclosed that affected Client Certificate authentication on all common web servers and browsers. The issue has been addressed by a change to the SSL protocol. Identity Manager has support for the updated protocol but many common browsers do not. To support browsers that have not been updated you can enable the previous behaviour.

This setting will apply to all web SSL connections to the server.

☒ Allow pre-CVE-2009-3555 SSL Renegotiation

- Click on the next button and then close.

Administrators can then apply certificates ready for sponsor use using Internet Options on the sponsor's browser. After the certificate has been successfully imported onto the browser, the sponsors can login automatically to the sponsor interface using an SSL connection.

Changing the Order of Authentication Servers

When a sponsor authenticates against FortiConnect it tries each authentication server that has been defined, in order, until it successfully authenticates a sponsor. If none of the authentication servers can authenticate the sponsor, an error message is returned.

As you can define many different authentication servers of different kinds, you can order them in any way you want on a server-by-server basis.

- From the administration interface, select Sponsor Portal > Authentication and click on the Authentication Servers Tab from the menu as shown below.

Order	Enabled	Name	Type	Server	Client Certificates	Single Sign On
1 ▼	●	10.10.1.2	RADIUS	10.10.1.2	n/a	n/a
2 ▲▼	●	10.10.1.2	Novell eDirectory	10.10.1.2	Configure	n/a
3 ▲▼	●	10.10.1.2	Generic LDAP	10.10.1.2	Configure	n/a
4 ▲▼	●	10.10.1.2	Microsoft Active Directory	10.10.1.2	Configure	Configure
5 ▲	●	Local	Internal sponsor database		n/a	n/a

[Add Server...](#)
[Save Order](#)
[Cancel](#)

The first server to be authenticated against is at the top of the list and the last one at the bottom.

- Select the server that you want to re-order from the list and click either the up or down button. Perform this action with all the servers until they are in the correct order.
- To save the authentication order click the Save Order button.

Network Access Policy

Authentication Policy

FortiConnect allows Users to be authenticated via either the internal User database or an external authentication server if required. For an authentication attempt against FortiConnect each server is tried in order against the relevant domain. If an external server rejects the authentication attempt then the user is rejected by FortiConnect. If a server does not respond the next server in the realm is tested.

Adding Authentication Servers

To add an external authentication server for Authentication go to Network Access Policy --> Authentication Policy from the FortiConnect Administration Interface.

Adding Authentication Servers

Authentication Policy

For every authentication the user credentials are verified in the following order:

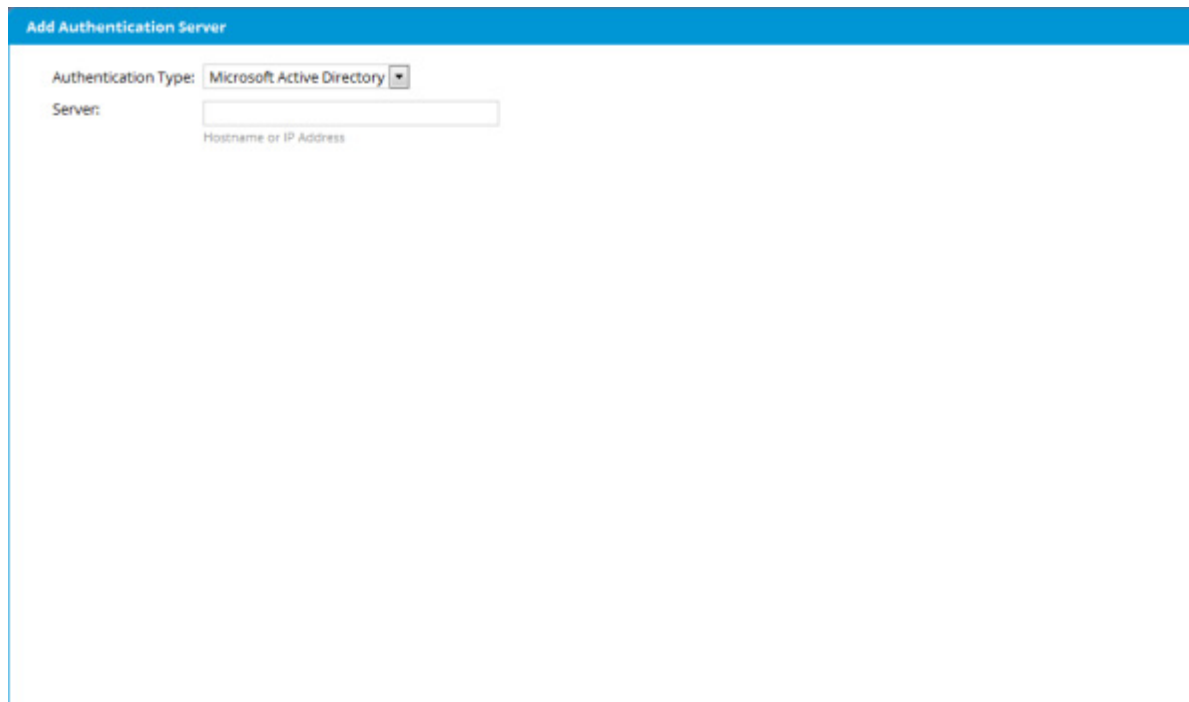
- Servers that match the realm of the user account. For example if the username was user@realm then the account would be verified against each server for that realm until a success or reject is received.
- If a Server does not respond, then the next server for the realm is tried.

Order	Enabled	Name	Type	Server	Realm
No authentication servers defined					

Add Server...Save OrderCancel

1. Click on the Add Server button and select what type of server you wish to add from the drop down menu provided

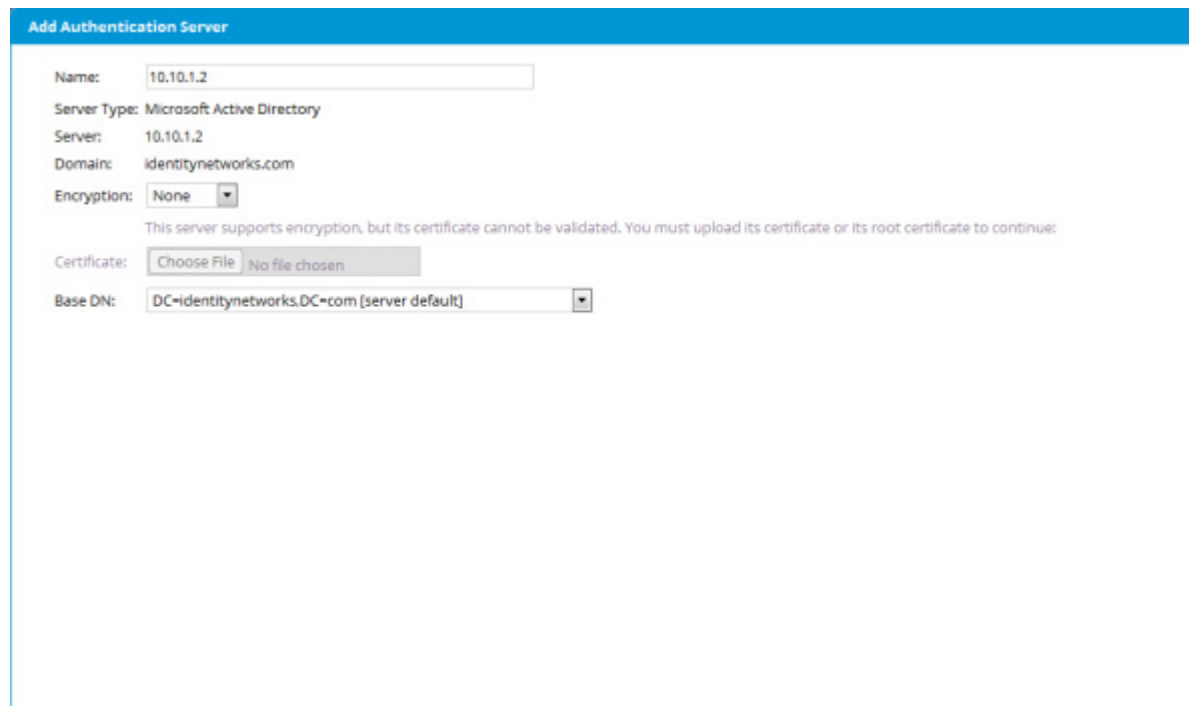
Note: For this example we will add a Microsoft Active Directory server, other parameters maybe required when adding other types of Authentication Servers



The screenshot shows the 'Add Authentication Server' form with the following fields:

- Authentication Type:** Microsoft Active Directory (dropdown menu)
- Server:** (text input field)
- Hostname or IP Address

2. Enter the hostname or IP address of the server and click on next



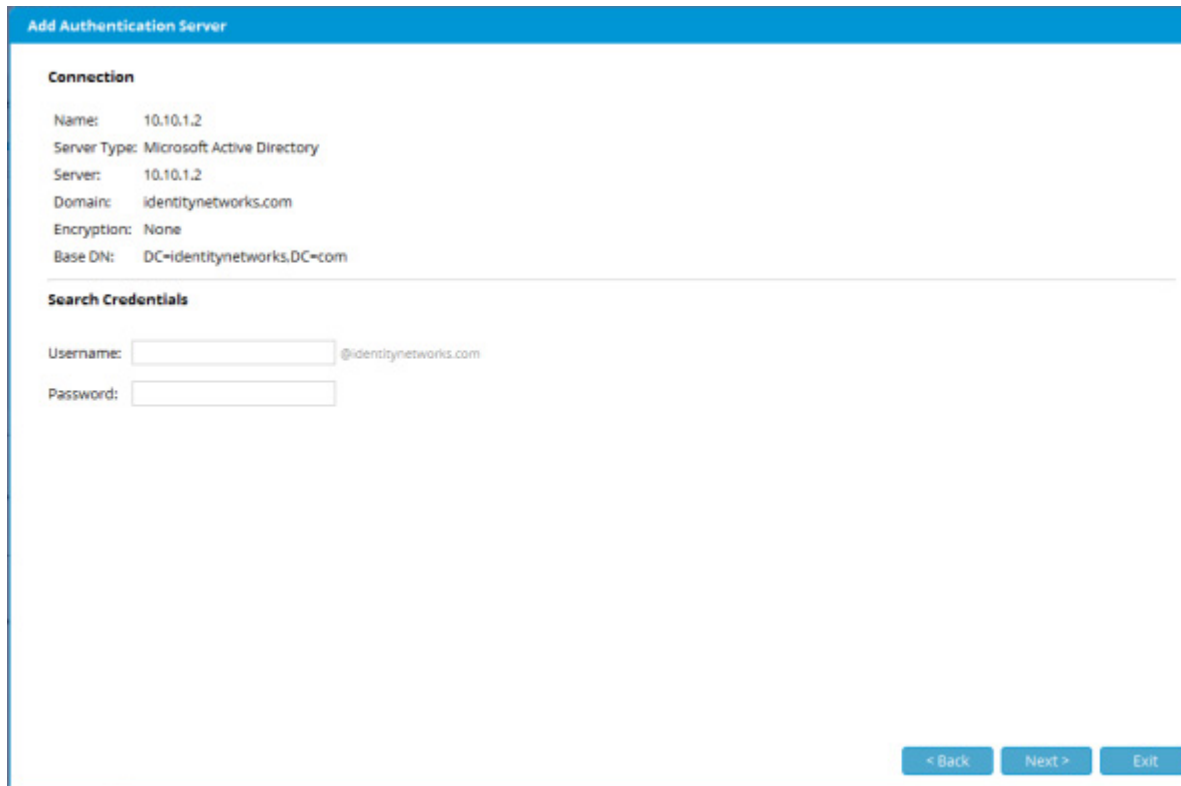
The screenshot shows the 'Add Authentication Server' form with the following fields:

- Name:** 10.10.1.2
- Server Type:** Microsoft Active Directory
- Server:** 10.10.1.2
- Domain:** identitynetworks.com
- Encryption:** None (dropdown menu)
- This server supports encryption, but its certificate cannot be validated. You must upload its certificate or its root certificate to continue:
- Certificate:** Choose File No file chosen
- Base DN:** DC=identitynetworks,DC=com [server default] (dropdown menu)

3. Select additional details from the drop down menus provided
 - Encryption - From the drop down menu select which encryption method the server will use.

Adding Authentication Servers

- Base DN - From the drop down menu select the Base DN the server will use from the options provided.
4. Click on Next and then enter the username and password of the server.



The screenshot shows a web-based configuration window titled "Add Authentication Server". It is divided into two main sections: "Connection" and "Search Credentials".

Connection

Name: 10.10.1.2
Server Type: Microsoft Active Directory
Server: 10.10.1.2
Domain: identitynetworks.com
Encryption: None
Base DN: DC=identitynetworks,DC=com

Search Credentials

Username: @identitynetworks.com
Password:

At the bottom right, there are three buttons: "< Back", "Next >", and "Exit".

5. Enter any attribute mappings required for the server and then map them to the usage profile you require and also set the Account Group.

Add Authentication Server

Connection
Name: 10.10.1.2
Server Type: Microsoft Active Directory
Server: 10.10.1.2
Domain: identitynetworks.com

Attribute Mappings

The response from the external server is tested against each rule below in order. If a rule is matched the specified usage profile and account group are applied and guest authentication succeeds.

1

If group name equals set usage profile to and account group to

2

If no rules match Reject authentication

[add mapping](#)

< Back

Next >

Exit

6. Autocomplete will assist you when entering your rules.
7. Continue to add rules and then click Next once complete.

Adding Authentication Servers

Add Authentication Server

Connection

Name: 10.10.1.2
Server Type: Microsoft Active Directory
Server: 10.10.1.2
Domain: identitynetworks.com

Secure Authentication

To enable MSCHAPv2 authentication from Windows clients this server must be joined to the AD domain. This is not required for EAP-TLS authentication.

This server is not joined to the domain.

[Join the domain](#) [Disconnect from the domain](#)

☐ Allow Windows computer authentication (machine/host authentication)

[< Back](#) [Next >](#) [Exit](#)

8. Place a check in Allow Windows computer authentication to allow the authentication server to allow machine/host authentication.
9. Click on the Join Domain to join the server to the domain as shown below.

The screenshot shows the 'Add Authentication Server' wizard. The 'Connection' section displays the following information:

- Name: 10.10.1.2
- Server Type: Microsoft Active Directory
- Server: 10.10.1.2
- Domain: identitynetworks.com

The 'Secure Authentication' section is partially visible, showing text about enabling MSCHAPv2 authentication. A modal dialog box titled 'Join server to domain' is overlaid on the screen. It contains the following fields and controls:

- Domain Administrator Username: [text input] @identitynetworks.com
- Password: [password input]
- A note: 'This password is only used to join this server to the Domain. It is not saved.'
- Buttons: 'Join' and 'Close'

At the bottom of the wizard, there are navigation buttons: '< Back', 'Next >', and 'Exit'.

10. Enter the Domain Administrator Username and Password then click on Join.

11. You will then be presented with a screen as shown below, this is to allow EAP-TLS authentication,

Adding Authentication Servers

Add Authentication Server

Connection

Name: 10.10.1.2
Server Type: Microsoft Active Directory
Server: 10.10.1.2
Domain: identitynetworks.com

EAP-TLS Authentication

Certificate Authorities: No Certificate Authorities defined

CA Certificates:

- ☐ Class 3 Public Primary Certification Authority
- ☐ Class 3 Public Primary Certification Authority - G2 (c) 1998 VeriSign, Inc. - F...
- ☐ DigiCert High Assurance CA-3
- ☐ DigiCert High Assurance EV Root CA
- ☐ Entrust Certification Authority - L1C
- ☐ Entrust.net Certification Authority (2048)
- ☐ Entrust.net Secure Server Certification Authority
- ☐ Equifax Secure Certificate Authority
- ☐ GeoTrust Global CA
- ☐ Thawte DV SSL CA

Upload a CA certificate: Choose File No file chosen

< Back Next > Exit

12. You will be required to determine your EAP-TLS Authentication method, if this does not apply to you, then click on next to complete setup.

- **Certificate Authorities** - FortiConnect allows you to define a SCEP server or to define an internal CA authority method. Any that have been setup within FortiConnect will be displayed in this drop down menu. Select your appropriate method.
- **CA Certificates** - Place a check in the check box next to any CA Certificates you wish to install.
- **Upload a CA Certificate** - Click on the choose file button and manually select a CA certificate to install.

13. Click Next to continue.

Note: If no certificates are installed then installation is now complete.

Add Authentication Server

To configure client certificates you can upload a sample user certificate. By inspecting this certificate the system will automatically determine how to map the client certificate to a user on an authentication server.

☒ Parse a sample PKCS#12 file

PKCS#12 File: No file chosen
Files usually end in a p12 or pkcs12 extension

Password:
The password is only used to extract the certificate from the PKCS#12 file. It is not stored.

☐ Parse a sample X.509 certificate in PEM or DER format

Certificate: No file chosen
Files usually end in a pem, cer, der or crt extension

14. To configure client certificates you can upload a sample user certificate. By inspecting this certificate the system will automatically determine how to map the client certificate to a user on an authentication server.
- Parse a sample PKCS#12 file - Select and browse to Parse a sample PKCS#12 file. Enter the relevant password and click next to continue.
 - Parse a sample X.509 certificate in PEM or DER format - Select and browse to Parse sample X.509 certificate in PEM or DER format and click next to continue.

Adding Authentication Servers

Sample Client Certificate

Common Name (CN):	John Carter
Subject DN:	/C=GB/ST=Greater Manchester/L=Manchester/O=Menu Networks/OU=Identity Manager/CN=John Carter/emailAddress=jcarter@merunetworks.com
Parsed Subject DN:	CN=John Carter,OU=Identity Manager,O=Menu Networks,L=Manchester,ST=Greater Manchester,C=GB
Email Address:	jcarter@merunetworks.com
User ID:	<Not part of certificate>
User Principal Name:	upn@identitynetworks.com

Find user on server by mapping Client Certificate to user attribute .

[Advanced >](#)

User Search Results

☒ User found

CN:	John Carter
DN:	CN=John Carter,CN=Users,DC=identitynetworks,DC=com
Email Address:	john@identitynetworks.com
Username:	john
User Principal Name:	john@identitynetworks.com

15. This will match the certificate with a user. Click on Next to continue.

Certificate Matching

Some authentication servers have the client certificate of each user. We can compare that certificate with the one supplied by the browser and the user will only be logged in if the certificates match.

This authentication server does not appear to store the user's certificate.

☐ Verify the user's certificate stored on the server matches the client certificate supplied by the browser.

16. Some authentication servers have the client certificate of each user. We can compare that certificate with the one supplied by the browser and the user will only be logged in if the certificate matches. To verify if the users certificate stored on the server matches the client certificate by the browser then place a check in the check box.

17. Click on Next to continue..

18. To allow secure connections from Windows clients the server must be added to the AD domain.

Note: FortiConnect supports MSCHAPv2 authentication so that a Windows client can connect to a controller that uses the FortiConnect as a RADIUS server that in turns authenticates against an Active Directory server.

FortiConnect supports authentication from users in domains that are trusted by the domain that FortiConnect is joined to, so if Domain A trusts Domain B, then users from Domain B can also be authenticated to the FortiConnect.

19. Once the server has been added click on Next and then click on the Close button.

External Database Authentication

FortiConnect allows an External Database to be configured for external authentication.

To add an external database for authentication go to Network Access Policy --> Authentication Policy from the FortiConnect Administration Interface.

Authentication Policy

For every authentication the user credentials are verified in the following order:

- Servers that match the realm of the user account. For example if the username was user@realm then the account would be verified against each server for that realm until a success or reject is received.
- If a Server does not respond, then the next server for the realm is tried.

Order	Enabled	Name	Type	Server	Realm
No authentication servers defined					

Add Server...

Save Order

Cancel

1. Click on the Add Server button and select External Database.

The screenshot shows a window titled "Add Authentication Server". Inside the window, there is a label "Authentication Type:" followed by a dropdown menu that currently displays "External Database". The rest of the window is empty. At the bottom right corner, there are three buttons: "< Back", "Next >", and "Exit".

2. Click on Next to continue.

External Database Authentication

Add Authentication server

Connection

Name:

Authentication type: External Database

Type:

Server IP Address:

Port:

Username:

Password:

Database Name:

Data Queries

- A user is authenticated if the authentication query returns a row.
- If any of the following columns are set in that row they are applied to the generated account: **first_name**, **last_name**, **email**, **phone** and **country_phone_code**.
- The optional group query shall return rows with a single column containing the group name.
- The groups are passed to the group mappings to determine the user's usage and authorization profiles.
- Query parameters **%username** and **%password** are required in the authentication query.
- Query parameter **%username** is required in the group query.

Authentication Query:

Group Query:

[Test Settings](#)

[Back](#) [Next](#) [End](#)

3. Enter the required credentials in the fields provided -
 - Name - Enter the name of your External Database
 - Type - From the drop down menu select the type of external database
 - Server IP Address - Enter the server IP Address
 - Port - Enter the required port number, leave blank to use the selected types default port
 - Username - Enter the required username
 - Password - Enter the required password
 - Database Name - Enter the database name
4. Define the Authentication Query and Group Query required to get user groups from the database.
5. Click on the Test Settings button to check your settings are correct.
6. Click on Next to continue.

Add Authentication Server

Connection
Name: Test Server
Authentication Type: External Database
Server: 10.10.1.2
Type: Microsoft SQL Server

Login Parameters
Realm:
Authenticates with: username

Group Mappings

The user group(s) returned by external database server is tested against each rule below in order. If a rule is matched the specified usage profile and account group are applied and guest authentication succeeds.

1
If group name equals set usage profile to and account group to

2
If no rules match Reject authentication

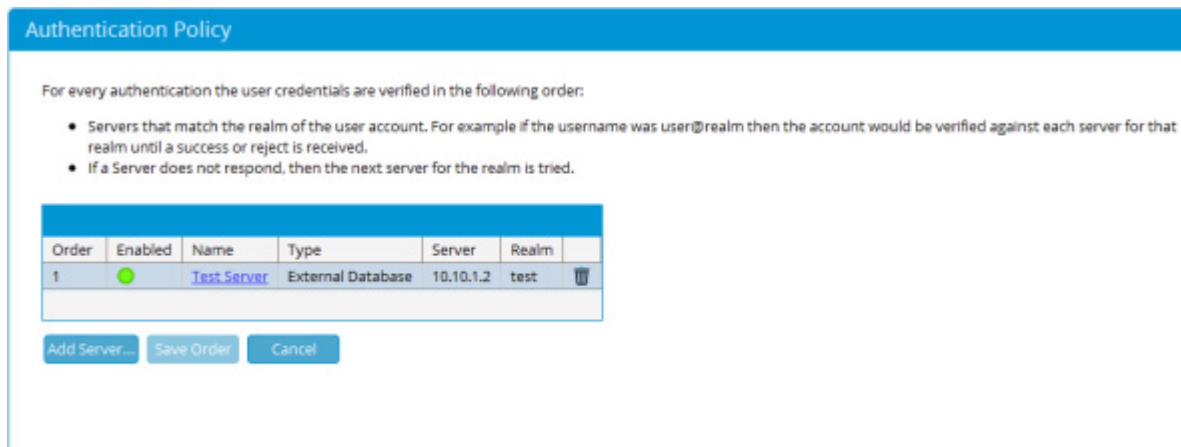
[add Rule](#)

< Back
Next >
Exit

7. Enter the Login Parameters required -
 - Realm - Enter the Realm
8. Enter the relevant Group Mappings required, each user group returned will be tested against each rule created in order.
9. Use the drop down menu to select and amend rules.
10. Click on the add rule link to add further rules.
11. Click Next once complete.
12. Click on Close to complete.

Deleting an External Authentication Server

To delete an External Authentication server once its has been added go to Network Access Policy --> Authentication Policy from the FortiConnect Administration interface



Click on the bin icon to the right of the server you wish to delete and click on yes at the prompt.

RADIUS and RadSec for Eduroam

Eduroam (education roaming) is the secure, world-wide roaming access service developed for the international research and education community.

Eduroam allows students, researchers and staff from participating institutions to obtain Internet connectivity across campus and when visiting other participating institutions by simply opening their laptop.



RADIUS and RadSec authentication servers can be added to support this feature.

To add a RADIUS or a RadSec authentication server go to Network Access Policy --> Authentication Policy from the FortiConnect Interface as shown below.

Authentication Policy

For every authentication the user credentials are verified in the following order:

- Servers that match the realm of the user account. For example if the username was user@realm then the account would be verified against each server for that realm until a success or reject is received.
- If a Server does not respond, then the next server for the realm is tried.

Order	Enabled	Name	Type	Server	Realm	
1		Test_Server	External Database	10.10.1.2	test	

[Add Server...](#) [Save Order](#) [Cancel](#)

1. Click on the Add Server button

Note: Only the first two screen shots differ for RADIUS and RadSec. For documentation purposes we will document the different screenshots, then continue with the setup which is the same for both RADIUS and RadSec from step 10 onwards

Selecting RADIUS

The screenshot shows a web-based configuration interface titled "Add Authentication Server". It features a blue header bar. Below the header, there is a form with two main sections. The first section, labeled "Authentication Type:", contains a dropdown menu currently showing "RADIUS". The second section, labeled "Server:", contains a text input field. Below this field, the text "Hostname or IP Address" is displayed as a hint. At the bottom right of the form, there are three buttons: "< Back", "Next >", and "Exit".

2. Enter the Hostname or IP Address of the RADIUS server.
3. Click on Next

Add Authentication Server

Name:

Authentication Type: RADIUS

Support eduroam: ☒ Authentication requests from unknown realms will be proxied to this server

Operation Mode:

Primary RADIUS server

Server IP Address:

Authentication Port:

Proxy Accounting: ☐

Accounting Port:

Secret: Confirm:

Secondary RADIUS server (Optional)

Server IP Address:

Authentication Port:

Proxy Accounting: ☐

Accounting Port:

Secret: Confirm:

4. Enter the relevant settings in the fields provided -

- Support Eduroam - Check the box to enable Eduroam support.
- Operation Mode - Use the drop down menu to determine whether the two servers should operate in failover mode or load balance mode.

Primary RADIUS Server

- Server IP Address - IP address of the server
- Authentication Port - Authentication Port number
- Proxy Accounting - Check the box to enable Proxy Accounting
- Accounting Port - Accounting Port number
- Secret - Enter and confirm the shared Secret

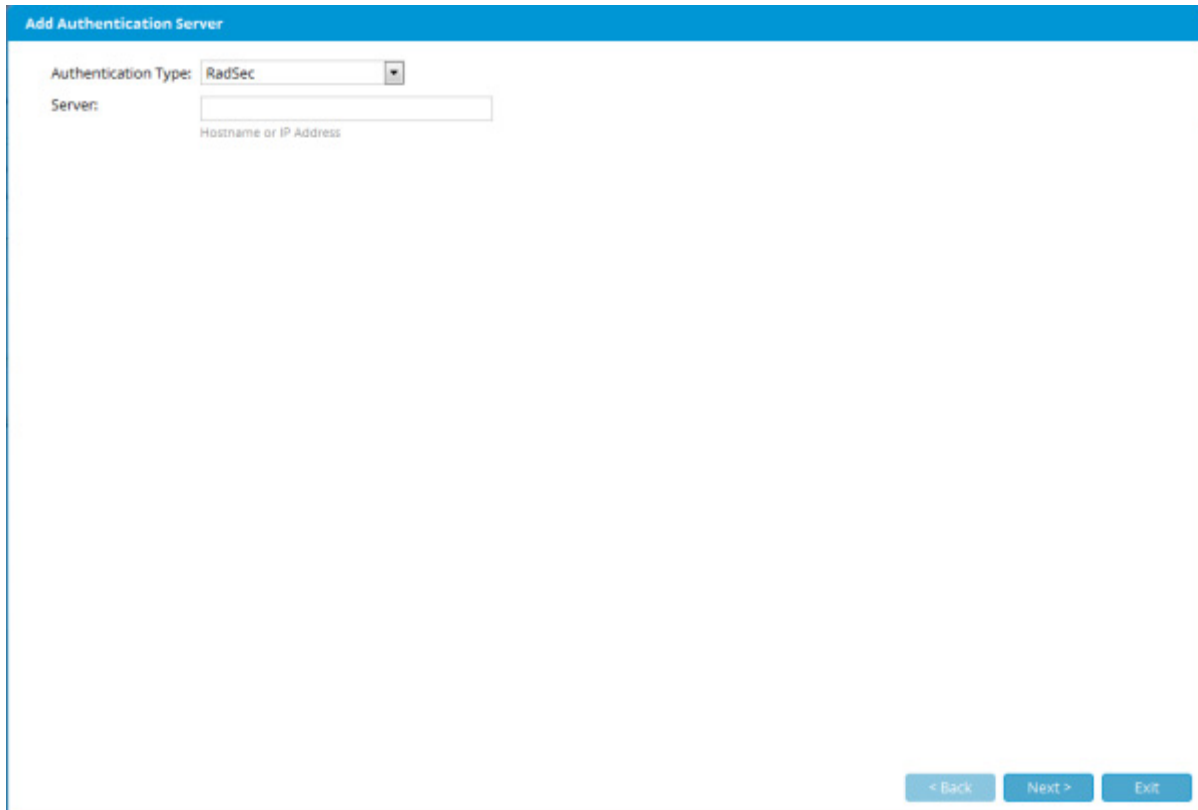
Secondary RADIUS Server (Optional)

- Server IP Address - IP address of the server
- Authentication Port - Authentication Port number
- Proxy Accounting - Check the box to enable Proxy Accounting

- Accounting Port - Accounting Port number
- Secret - Enter and confirm the shared Secret

5. Click on Next to continue and go to step 10.

Selecting RadSec



The screenshot shows a web-based configuration interface titled "Add Authentication Server". It features a blue header bar. Below the header, there is a form with the following elements:

- Authentication Type:** A dropdown menu currently showing "RadSec".
- Server:** A text input field that is currently empty.
- Placeholder text:** Below the "Server" field, the text "Hostname or IP Address" is displayed in a smaller font.
- Navigation buttons:** At the bottom right of the form, there are three buttons: "< Back", "Next >", and "Exit".

6. Enter the Hostname or IP Address of the RadSec server.
7. Click on Next

Add Authentication Server

Name: 10.10.1.2

Authentication Type: RadSec

Support eduroam: ☒ Authentication requests from unknown realms will be proxied to this server

Primary RadSec server

Server: 10.10.1.2
Hostname or IP Address

Verify SSL Certificate CN: ☒

RadSec Type: TLS

Authentication Port: 2083

Secret: Confirm:

Proxy Accounting: ☐

Failover RadSec server (Optional)

Server:
Hostname or IP Address

Verify SSL Certificate CN: ☒

RadSec Type: TLS

Authentication Port: 2083

Secret: Confirm:

Proxy Accounting: ☐

< Back Next > Exit

8. Enter the relevant settings in the fields provided -

- Support Eduroam - Check the box to enable Eduroam support.

Primary RadSec Server

- Server - Enter the hostname or IP address of the server
- Verify Certificate CN - Enable this checkbox to enable verification
- RadSec Type - From the drop down menu select TLS or DTLS as RadSec type
- Authentication Port - Enter the Authentication port number (If Support Eduroam was selected then this option will not be available)
- Secret - Enter then confirm the shared secret (If Support Eduroam was selected then this option will not be available)
- Proxy Accounting - Check to enable proxy accounting

Failover RadSec Server (Optional)

- Server - Enter the hostname or IP address of the server
- Verify Certificate CN - Enable this checkbox to enable verification

- **RadSec Type** - From the drop down menu select TLS or DTLS as RadSec type
- **Authentication Port** - Enter the Authentication port number (If Support Eduroam was selected then this option will not be available)
- **Secret** - Enter then confirm the shared secret (If Support Eduroam was selected then this option will not be available)
- **Proxy Accounting** - Check to enable proxy accounting

9. Click on Next to continue and go to step 10.

10. You should now see the screen below, the next steps are applicable to both RADIUS and RadSec setup.

- **Vendor** - Enter the relevant Vendor from the drop down list
- **Authenticate with** - Select the relevant username format

11. Now you can add any attributes you wish to inject into RADIUS requests sent to the RADIUS server

- **Vendor** - From the drop down menu select which vendor is required

- Attribute - Select an attribute from the drop down menu
- Value - Enter the required value
- Add AV Pair - Click to add your pairing to the list.
- Use the Buttons on the right hand side of your list to order your attributes, click on remove to remove an attribute.

12. To add a mapping click on the add mapping link and create your rule as shown below.

Add Authentication Server

Connection

Name: 10.10.1.2
Server Type: RADIUS
Server: 10.10.1.2

Login Parameters

Realm: eduroam
Authenticate with: ☐ eduroam\username
☐ eduroam/username
☒ username@eduroam
☐ username
Enable SSID Mapping: ☐

Attribute Mappings

The response from the external server is tested against each rule below in order. If a rule is matched the specified usage profile and account group are applied and guest authentication succeeds.

1
If attribute equals
set usage profile to
and account group to

2
If no rules match Reject authentication

[add mapping](#)

< Back
Next >
Exit

13. Click Next to continue.

Add Authentication Server

Please select the CA certificates that should be used to validate this server.

- ☐ Class 3 Public Primary Certification Authority
- ☐ Class 3 Public Primary Certification Authority - G2 (c) 1998 VeriSign, Inc. - For authorized use only VeriSign Trust Network
- ☐ DigiCert High Assurance CA-3
- ☐ DigiCert High Assurance EV Root CA
- ☐ Entrust Certification Authority - L1C
- ☐ Entrust.net Certification Authority (2048)
- ☐ Entrust.net Secure Server Certification Authority
- ☐ Equifax Secure Certificate Authority
- ☐ GeoTrust Global CA
- ☐ Thawte DV SSL CA
- ☐ Thawte Premium Server CA
- ☐ Thawte SGC CA
- ☐ VeriSign Class 3 Public Primary Certification Authority - G5
- ☐ VeriSign Class 3 Secure Server CA - G2
- ☐ VeriSign Class 3 Secure Server CA - G3
- ☐ localhost.localdomain [localhost]

Upload Certificate:

14. Now select the CA certificates that should be used to validate your server, choose from the list provided or upload a certificate using the Choose File option.

15. Click Next once complete.

16. You have now successfully added an authentication server for RADIUS/RadSec Eduroam support.

Authorization Policy

Authorization Policy enables you to give different authorization to users on different devices. For example allowing users on corporate devices to access internal resources, while giving users on personal devices less access to sensitive data – maybe allowing access only to the internet.

Administrators can add devices to a list using their MAC address as the identifier and then write a policy so that upon a RADIUS authentication the system can assign a different authorization if the calling-station-id (MAC Address) is in the admin defined list.

Adding an Authorization Policy

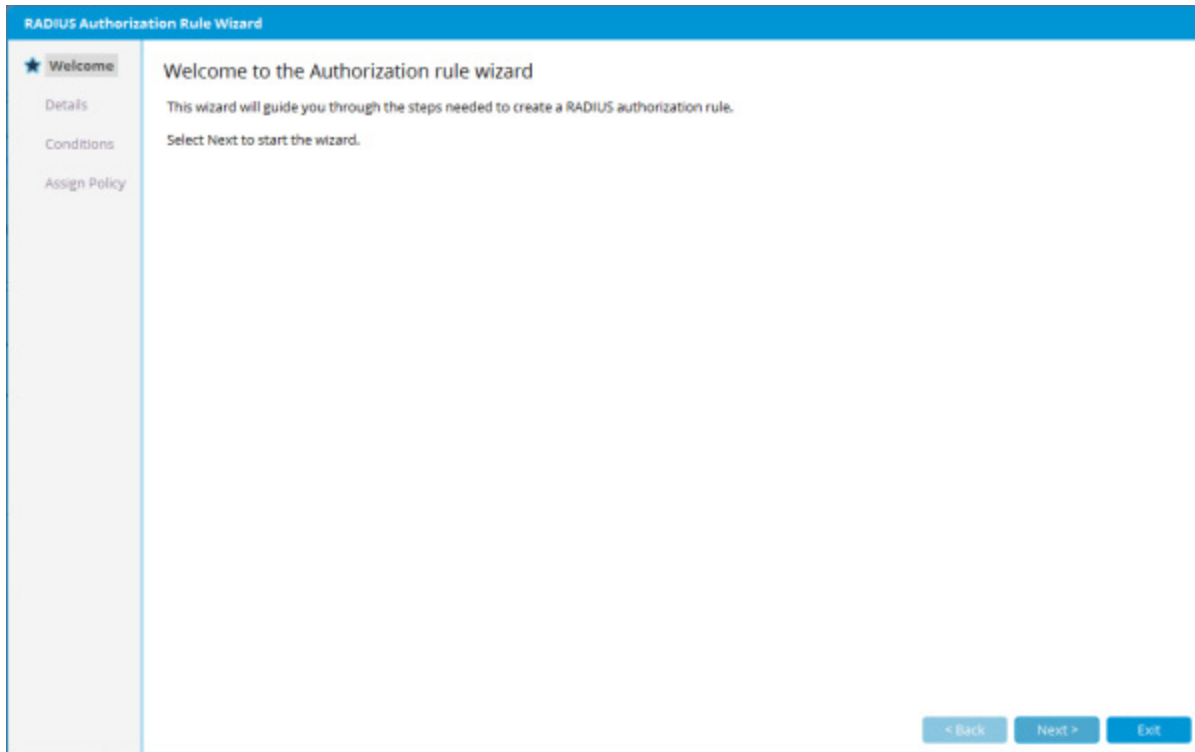
1. From the FortiConnect Administration Interface go to Network Access Policy --> Authorization Policy as shown below.

Order	Name	Rule	Authorization Profile	Enabled	Action
1	Default	Apply profile	Default	●	

[Save Order](#) [Add](#)

2. Each Authorization Policy is checked in the order displayed on the screen, if no policies match then the default policy will be applied
3. To add another Authorization Policy click on the Add button which will launch the Authorization Rule Wizard and then click on Next.

T



4. Enter a Name and Description of your Rule as shown below.

The screenshot shows the 'RADIUS Authorization Rule Wizard' window. On the left is a sidebar with four steps: 'Welcome' (checked), 'Details' (selected with a star icon), 'Conditions', and 'Assign Policy'. The main area is titled 'Rule Name' and contains two input fields: 'Name:' and 'Description:'. At the bottom right are three buttons: '< Back', 'Next >', and 'Exit'.

RADIUS Authorization Rule Wizard

✓ Welcome
★ **Details**
Conditions
Assign Policy

Rule Name

Name:

Description:

< Back Next > Exit

5. You will then be required to enter all the conditions that need to be met, click on Next to do this.

The screenshot shows the 'RADIUS Authorization Rule Wizard' interface. On the left is a sidebar with a vertical list of steps: 'Welcome' (checked), 'Details' (checked), 'Conditions' (selected with a star icon), and 'Assign Policy'. The main area is titled 'Rule Conditions' and contains the text 'All the conditions below must be met for this rule to match.' Below this text is a single condition: 'If account-group equal to [dropdown] Default Account Group [dropdown]'. A blue link labeled 'Add Condition' is positioned below the condition. At the bottom right of the main area are three buttons: '< Back', 'Next >', and 'Exit'.

6. The Default Rule Condition will initially be displayed, this can be deleted or amended as necessary.
7. To create a new rule condition, click on the Add Condition link.
8. This will then display an attribute link, click on that to select the attribute for the rule as shown below.

RADIUS Authorization Rule Wizard

✓ Welcome
✓ Details
★ **Conditions**
Assign Policy

Rule Conditions

All the conditions below must be met for this rule to match.

- If account-group equal to Default Account Group
- If account-group

[Add Condition](#)

Select Attribute

Type: Identity

Identity: IDM Account Group

Set Cancel

< Back Next > Exit

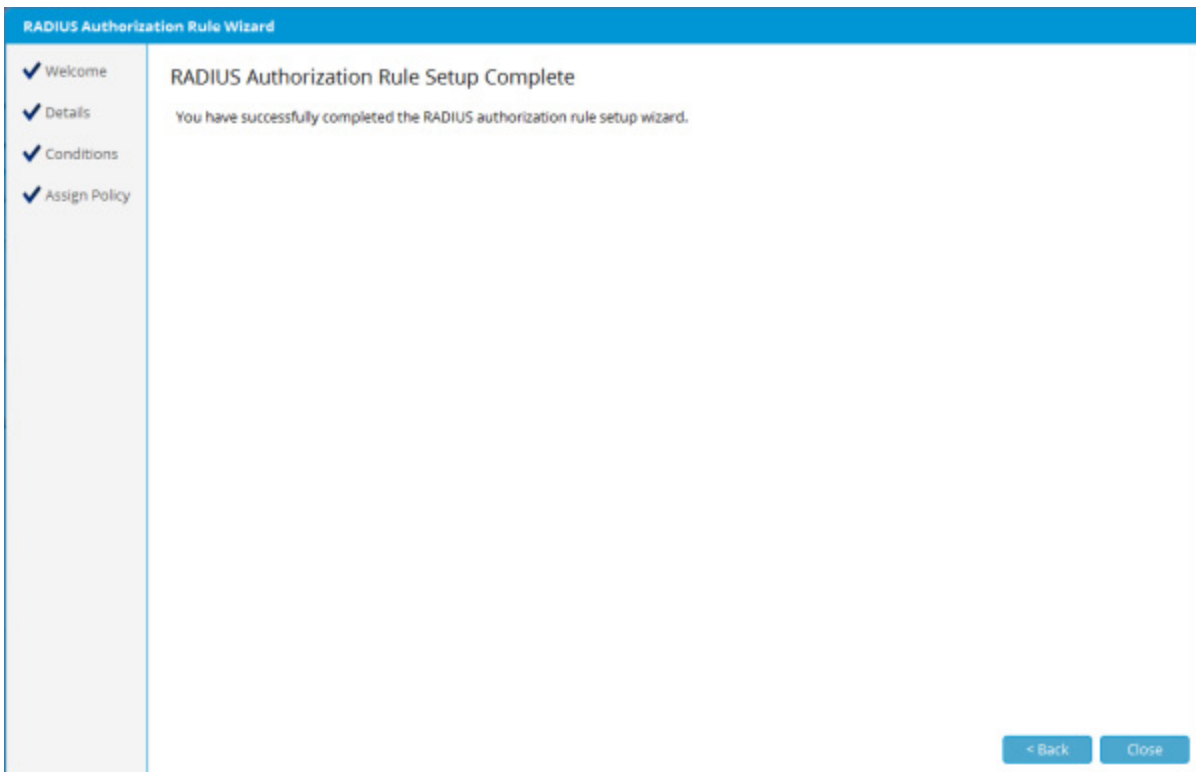
9. From the drop down menu select the Attribute type and then choose from -
 - RADIUS - Selecting RADIUS will then require you to enter Vendor and Attribute Types for your rule condition
 - Identity - Selecting Identity will then require you to select from an Account Group or a Group Membership for your rule condition
 - Time - Selecting Time will then require you to select Day Of Week or Time Of Day criteria for your rule condition
 - MDM - Selecting MDM will then require you to enter Vendor and Attribute Types for your rule condition
10. Click on Set once complete.
11. Enter any remaining conditions you require then click on Next when complete.
12. You should now select an authorization profile you want to assign to the users/devices that matches the authorization rule as shown below. Profiles can set up in Network Access Policy --> Authorization Profiles.

The screenshot shows the 'RADIUS Authorization Rule Wizard' with the 'Policy' step selected. The left sidebar contains a list of steps: 'Welcome', 'Details', 'Conditions', and 'Assign Policy' (which is highlighted with a star). The main area is titled 'Policy' and contains the instruction: 'Select the profile that you want to assign to users/devices that match this authorization rule.' Below this, there are two radio button options: 'Assign Profile' (which is selected) and 'No access (send RADIUS reject)'. The 'Assign Profile' option has a dropdown menu showing 'Default'. At the bottom right, there are three buttons: '< Back', 'Next >', and 'Exit'.

13. Select the appropriate Action :-

- Assign Profile - from the drop down menu select the profile that matches the authorization rule.
- No Access - select this to prevent users which match this policy from accessing the network

14. Click on Next to complete the Setup.



Editing an Authorization Policy

1. From the FortiConnect Administration Interface go to Network Access Policy --> Authorization Policy as shown below.

Authorization Policy

Authorization Policy

Each Authorization policy is checked in the following order. First matched policy is applied and no other policies are checked.

Order	Name	Rule	Authorization Profile	Enabled	Action
1	Connect Rule	account-group equals Default Account Group and account-group equals Default Account Group	Default		
2	Default	Apply profile	Default		

Save OrderAdd




2. Click on the Edit icon to the right of the policy you wish to Edit.
3. Repeat steps 6 - 13 in the Add Authorization Policy section above to make your changes.

Deleting an Authorization Policy

1. From the FortiConnect Administration Interface go to Network Access Policy --> Authorization Policy as shown below.

Authorization Policy

Each Authorization policy is checked in the following order. First matched policy is applied and no other policies are checked.

Order	Name	Rule	Authorization Profile	Enabled	Action
1	Connect Rule	account-group equals Default Account Group and account-group equals Default Account Group	Default	●	 
2	Default	Apply profile	Default	●	

2. Click on the Bin icon to remove the profile you wish to delete.
3. Click on Yes to confirm.

MDM Servers

FortiConnect can now integrate with MDM Vendors, current supported vendors are -

- Xenmobile
- Airwatch

An MDM server can be added, then Authorization Policies created with rules based on the MDM integration by going to Network Access Policy --> Authorization Policy from the FortiConnect Admin interface.

To add an MDM server, go to Devices --> MDM Servers as shown on the screen below.

MDM Servers

MDM Servers

Name	Description	Vendor	Enabled	Action
No MDM servers defined				

Add MDM Server

1. Click on the Add MDM Server button to enter the MDM Server details as shown below

Add New MDM Server

Server Name:

Server Description:

Vendor:

AirWatch

Server:

Validate Certificate:

☒

Username:

Password:

Confirm:

API Key:

Save

Cancel

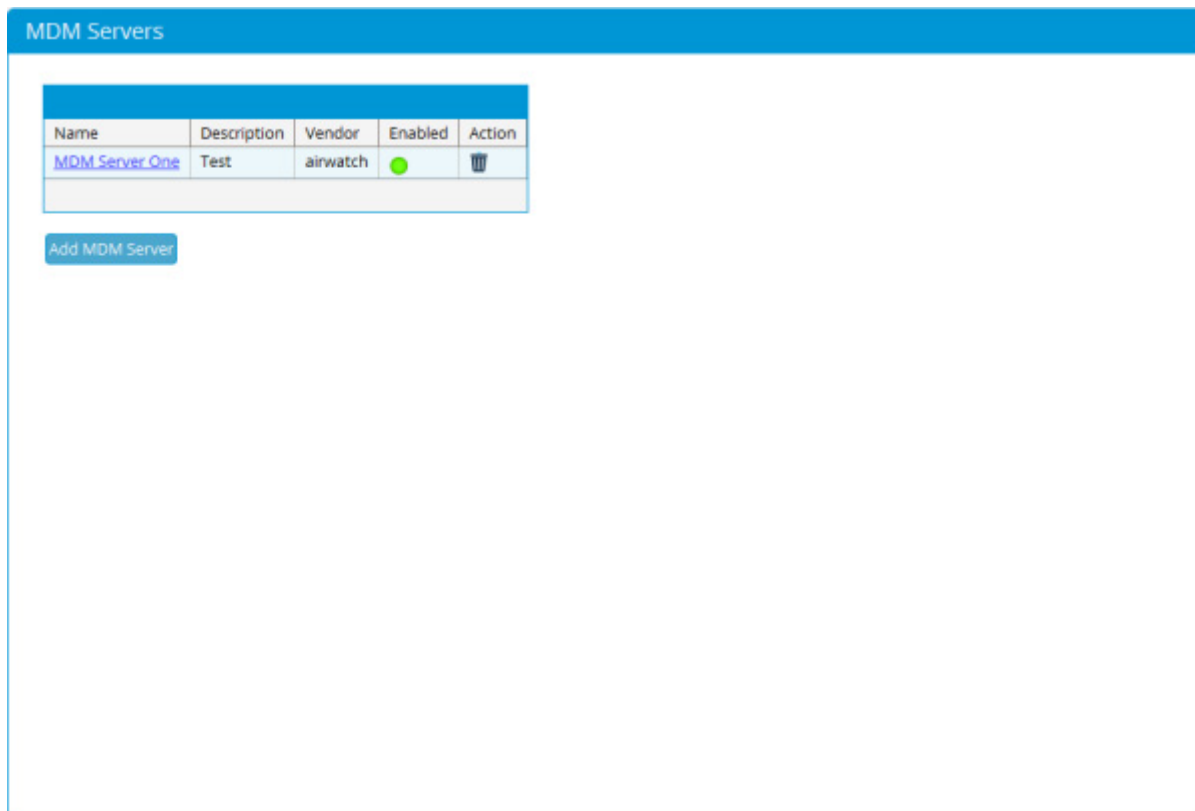
2. Now enter your Server details -

- **Server Name** - Enter the MDM server name
- **Server Description** - Enter the description of the MDM server
- **Vendor** - From the drop down menu select which Vendor of MDM server you wish to integrate with
- **Server** - Enter the IP address or the hostname of the server
- **Validate Certificate** - Check this box to validate the SSL cert on the server (CA certs must be installed on the FortiConnect for this to work)
- **Username** - Enter the username of the MDM server
- **Password** - Enter the password of the MDM server and confirm it
- **Tenant Code** - Enter the Tenant Code of the MDM server

3. Click on Save once complete

Edit an MDM Server

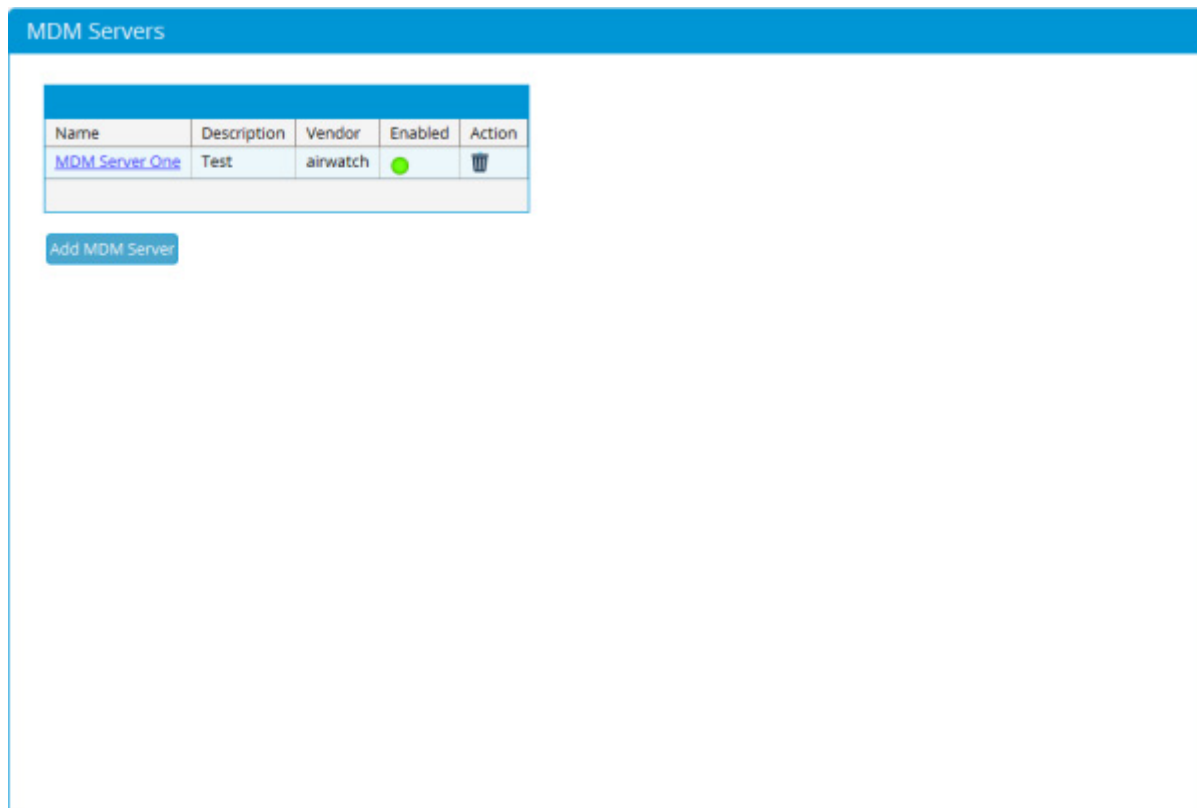
To Edit an MDM Server go to Devices --> MDM Servers as shown on the screen below.



1. Click on the Name of the MDM Server you wish to Edit and perform any necessary changes.
2. Click on Save once complete.

Deleting an MDM Server

To Delete an MDM Server go to Devices --> MDM Servers as shown on the screen below.



1. Click on the Bin Icon next to the MDM Server you wish to delete.
2. Click on Ok to confirm deletion.

Wi-Fi Based Marketing Notification Services

FortiConnect introduces support for 3rd party Wi-Fi based marketing notification services. Wi-Fi Based marketing notification services enables merchants to push promotions and other related notifications to customers in their close proximity.

How This Works

In FortiConnect, add the server / services details of the notification service provide. After adding this service, enable it in the Guest Portal settings. Any user authenticating via the IDM guest portal login will start seeing the notifications pushed from the server enabled in Guest Portal Settings.

Note: Only one server can be enabled per portal. Guest users will receive promotions from the server that is enabled in the guest portal and used by the guests to login

Adding and Configuring the Service

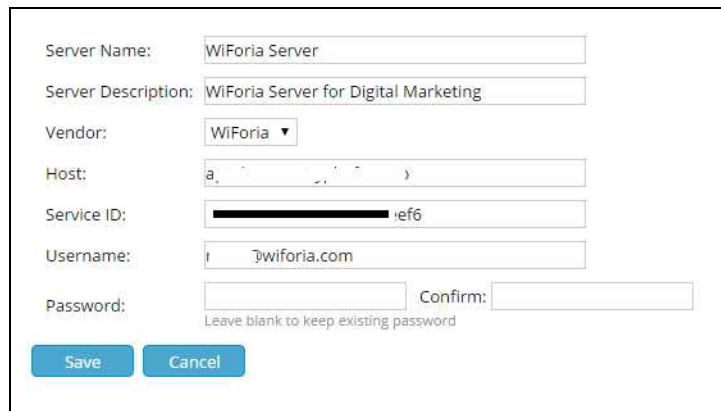
1. Login to FortiConnect Administration UI and go to Devices > WiFi Marketing Providers.



2. Click Add New Server to add a new service provider and enter the following details:

Field Name	Description
Server Name	Specify a name to identify the service provide. For ease of use, use the actual name of the service provider
Server Description	Specify additional information about the service provider
Vendor	Select the vendor from the list. NOTE: This release supports only WiForia
Host	Enter the IP address or domain name provided by the service provider
Service ID	This is provided by the service provider and is used to authenticate FortiConnect in their server

Field Name	Description
Username	This is provided by the service provider
Password	This is provided by the service provider



The screenshot shows a configuration form for a WiForia Server. The fields are as follows:

- Server Name:** WiForia Server
- Server Description:** WiForia Server for Digital Marketing
- Vendor:** WiForia (selected from a dropdown menu)
- Host:** a. (partially visible)
- Service ID:** ef6
- Username:** @wiforia.com
- Password:** (empty field) **Confirm:** (empty field)

Below the password fields is a note: "Leave blank to keep existing password". At the bottom are two buttons: "Save" and "Cancel".

3. After adding server details, click the SAVE button to continue.

In the Portal settings page, enable Wi-Fi marketing service. Go to Portals. You can select an existing portal or create a new one. If you already have portal to which you plan to enable the Wi-Fi marketing service, do the following:

Click an existing portal to open the Portal Settings Wizard. Click the Next button to navigate to the Portal Settings section. In this section, select WiFi Marketing Integration option to enable notification services.

★ Portal Settings

Portal Policy

Page	Displayed in menu	
	Pre-Authentication	Post-Authentication
Login	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Password Change	<input type="checkbox"/>	<input type="checkbox"/>
Self Service	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Device Registration	<input type="checkbox"/>	<input type="checkbox"/>
Credit Card Billing	<input type="checkbox"/>	<input type="checkbox"/>
Successful Authentication	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Welcome Back	<input type="checkbox"/>	<input type="checkbox"/>
Smart Connect	<input type="checkbox"/>	<input type="checkbox"/>
PMS Billing	<input type="checkbox"/>	<input type="checkbox"/>
Access without Login	<input type="checkbox"/>	<input type="checkbox"/>
Password Recovery	<input type="checkbox"/>	<input type="checkbox"/>
My Account	<input type="checkbox"/>	<input type="checkbox"/>
Help	<input type="checkbox"/>	<input type="checkbox"/>
Welcome	<input type="checkbox"/>	<input type="checkbox"/>

Session Management

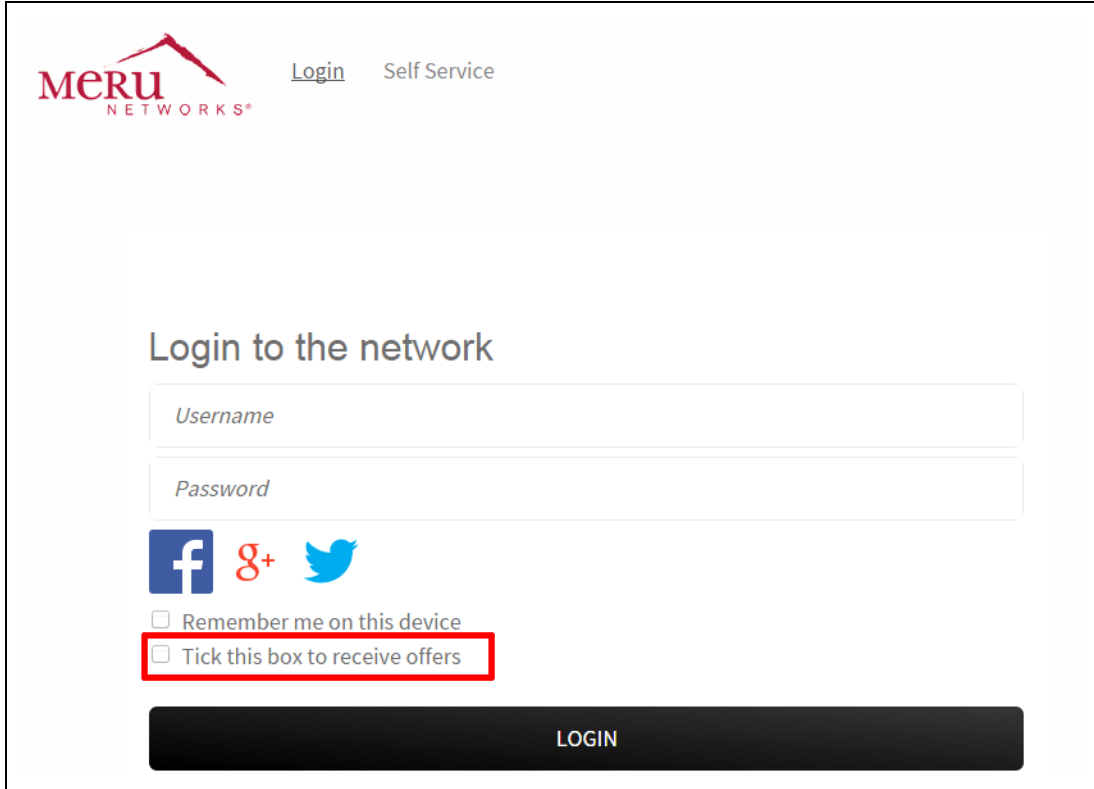
Allow user to close existing sessions when the concurrent session limit is exceeded: ☒

WiFi Marketing Integration

Enable WiFi Marketing Integration: ☒

For the Users

To receive notifications from the service providers, users login in using the captive portal page, must opt-in to receive notifications.



The screenshot shows the Meru Networks captive portal login interface. At the top left is the Meru Networks logo. To its right are links for 'Login' and 'Self Service'. The main heading is 'Login to the network'. Below this are two input fields: 'Username' and 'Password'. Under the password field are social media icons for Facebook, Google+, and Twitter. Below the icons are two checkboxes: 'Remember me on this device' and 'Tick this box to receive offers'. The second checkbox is highlighted with a red rectangular border. At the bottom is a large black button labeled 'LOGIN'.

Limitations

1. When a guest moves from one AP to another (change in location), FortiConnect can notify WiForia of this change only after 10 minutes, as the Controller will do the radius update only after 10 minutes (this can be changed based on the configuration in the controller, minimum value is 10 minutes).
2. The feature will work only for users who would do Self Service. i.e feature will not work for Guest accounts created by Sponsor.
3. Feature will not work for guests who authenticate with their Twitter accounts as Twitter will not send us the email address of the guest user.
4. This feature will not work for Mac authentication as Controller does not send Radius Accounting for this.

Configuring Authorization Profiles

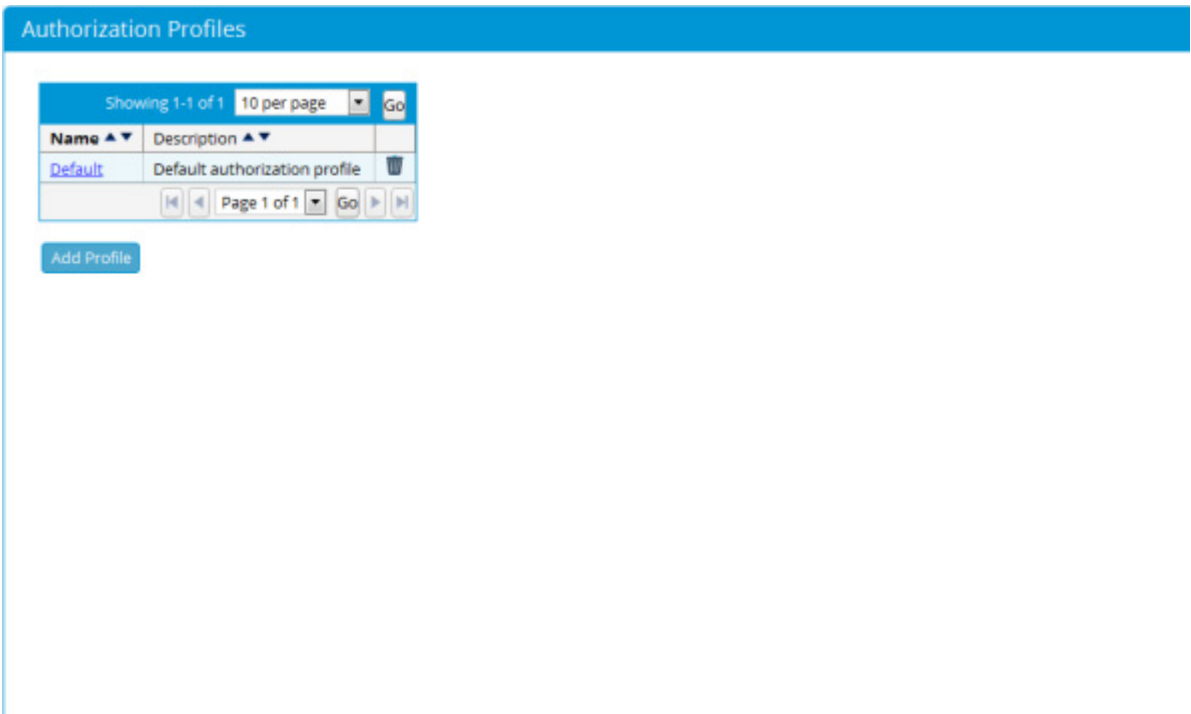
Authorization Profiles provide a way to give different levels of access to different accounts. For example, to assign different RADIUS attributes, or to only allow access to users from certain IP address ranges.

Once Authorization Profiles have been created, you must change the sponsor group to allow sponsors in that group to be able to provision accounts in the appropriate role.

Adding Authorization Profiles

You can add a new Authorization Profile using the following steps.

1. From the administration interface, select Network Access Policy > Authorization Profiles as shown below.



2. Click the Add Profile button to add a new Profile.
3. From the Add Profile page as shown below, enter the name for a new Authorization Profile.

Portal Setup Wizard

- ✓ Welcome
- ✓ Portal Name
- ✓ Portal Theme
- ★ **Portal Settings**
- Portal Policy

Portal Pages

Specify which pages your portal should have enabled and at what stage they should be available.

Page	Displayed in menu	
	Pre-Authentication	Post-Authentication
Login	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Password Change	<input type="checkbox"/>	<input type="checkbox"/>
Self Service	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Device Registration	<input type="checkbox"/>	<input type="checkbox"/>
Credit Card Billing	<input type="checkbox"/>	<input type="checkbox"/>
Successful Authentication	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Welcome Back	<input type="checkbox"/>	<input type="checkbox"/>
Smart Connect	<input type="checkbox"/>	<input type="checkbox"/>
PMS Billing	<input type="checkbox"/>	<input type="checkbox"/>
Access without Login	<input type="checkbox"/>	<input type="checkbox"/>
Password Recovery	<input type="checkbox"/>	<input type="checkbox"/>
My Account	<input type="checkbox"/>	<input type="checkbox"/>
Help	<input type="checkbox"/>	<input type="checkbox"/>
Welcome	<input type="checkbox"/>	<input type="checkbox"/>

Session Management

Allow user to close existing sessions when the concurrent session limit is exceeded: ☒

WiFi Marketing Integration

Enable WiFi Marketing Integration: ☐

Logout Options

Enable Logout Button: ☒

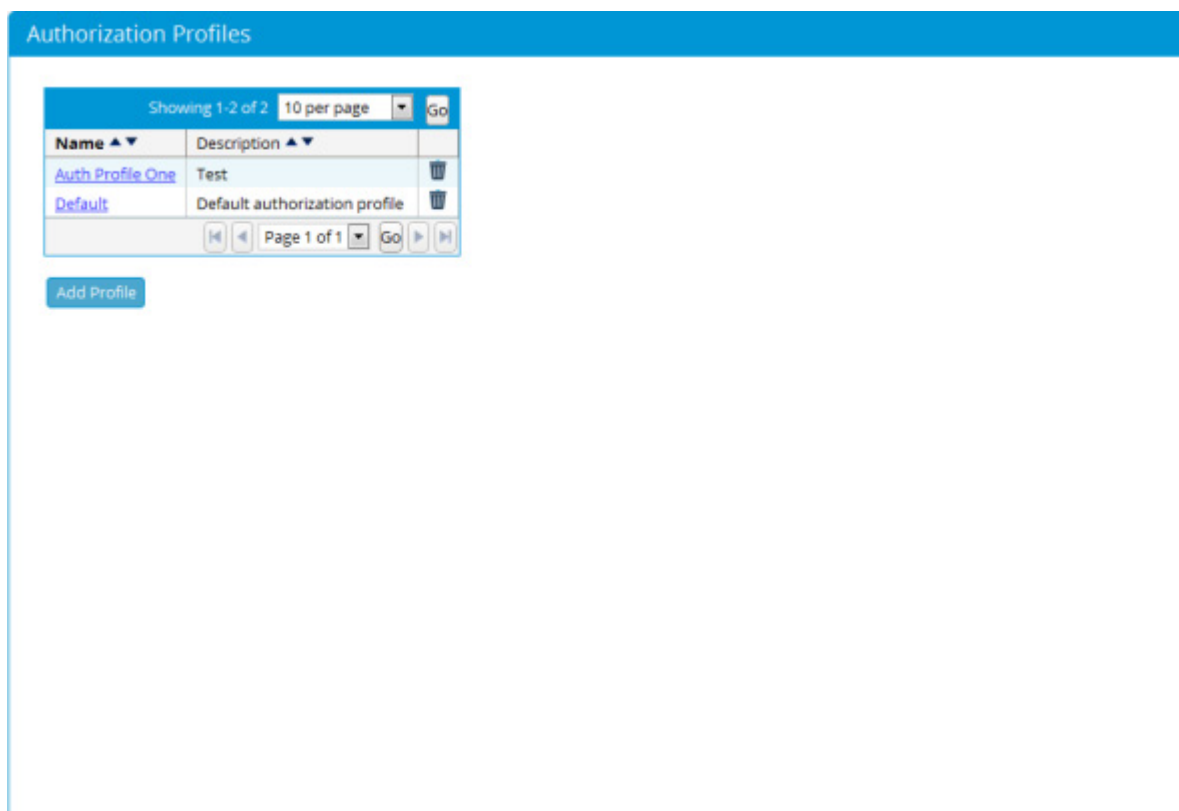
Enable Logout Pop-up window: ☒

4. Enter a Profile Name and its Description in the fields provided.
5. Click the Add Profile button to add the guest role. You can now edit the settings for the new guest role as described in Editing Authorization Profiles.

Editing Authorization Profiles

The following steps describe how to edit the profiles.

1. From the administration interface, select Network Access Policy > Authorization Profiles from the left hand menu.



2. Select the profile you wish to edit and click the underlined name of that profile as shown above to bring up the Edit Profiles page. From there you can edit the following attributes:
 - Edit RADIUS Attributes
 - Edit Locations
 - Edit Notification Settings
 - Edit Device Restrictions
 - Edit Auto MAC Registration

Edit RADIUS Attributes

If a User authenticates using a RADIUS client device such as a Wireless LAN controller, then for each role you can specify additional RADIUS attributes that are sent upon successful authentication.

1. From the administration interface, select Network Access Policy > Authorization Profiles and click the underlined name of that role you want to edit.
2. Select RADIUS Attributes from the tab at the top of the page as shown below.

Authorization Profiles: Auth Profile One

RADIUS Attributes | Locations | Notification Settings | Device Restrictions | Auto-MAC Registration

Vendor: IETF

Attribute: Access-Loop-Encapsulation

Value:

Add AV Pair

Move up
Remove
Move down

Save Cancel

3. From the drop down menu select the appropriate Vendor from the list.
4. If the selected Vendor has been successfully highlighted in step 3, then the Attribute field will auto-populate with the appropriate Attributes for that Vendor, select the desired Attribute from the drop down menu.
5. Enter the Value in the field provided.
6. Click on Add AV Pair
7. If you need to re-order the attributes that are sent, use the Move up and Move down buttons.
8. Click the Save button to save the RADIUS Attributes.

Edit Locations

If a User authenticates using a RADIUS client device such as a Wireless LAN Controller, you can specify from which IP address ranges the User is allowed to authenticate for each profile. This enables you to specify profiles based upon location so that Users assigned to a specific profile can only login from locations that you specify.

1. From the administration interface, select Network Access Policy > Authorization Profiles and click the underlined name of that profile you want to edit.
2. Click the Locations tab as shown below.

Authorization Profiles: Auth Profile One

RADIUS Attributes Locations Notification Settings Device Restrictions Auto MAC Registration

Locations only apply to RADIUS Authentication

IPv4 Network Address: /

0.0.0.0/0 Remove

Add Location Cancel

IPv6 Network Address: /

::/0 Remove

Add Location Cancel

3. Enter each Network Address and select the appropriate prefix length from the dropdown menu. Only valid Network Addresses will be accepted—host addresses must be specified using a /32 prefix length.
4. If your network uses IPv6 networking addresses then please use the section provided.
5. Click the Add Location button to add the Network Address.

Note: When you add a profile, the location 0.0.0.0/0 is automatically added. This means that the profile is valid from any IP address. If you want to restrict to other IP address ranges you must remove this address.

Note: Locations only apply to Users authenticating through RADIUS clients such as the Wireless LAN Controller.

Note: This only works when the RADIUS Client sends the Users IP address in the RADIUS authentication. The IP address must be contained in the Framed-IP-Address attribute.

Edit Notification Settings

Admin can configure the User Profile to send an Email and SMS notification after a User first logs on and to also send an expiry notification before a User Account expires.

1. From the FortiConnect administration interface, go to Network Access Policy --> Authorization Profiles and click on the Notification Settings tab as shown below.

The screenshot shows the 'Authorization Profiles: Auth Profile One' configuration page. The 'Notification Settings' tab is selected, showing options for SMS and Email notifications. The 'At Login' section has checkboxes for both SMS and Email, which are checked. Below these are input fields for 'Minutes since last login' and a note to 'Leave blank to send SMS/email at every login'. The 'Expiry' section also has checked checkboxes for SMS and Email, with corresponding 'Minutes before expiry' input fields. A 'Language Template' dropdown menu is set to 'English (Default)'. At the bottom are 'Save' and 'Cancel' buttons.

2. To enable an SMS Notification At Login, place a check in the Enable box and then specify how often you wish to send notifications. Leave blank to send an SMS at every login
3. To enable Email Notification At Login, place a check in the Enable box and then specify how often you wish to send notifications. Leave blank to send an email at every login
4. To enable an SMS Notification before Expiry, place a check in the Enable box and specify how many minutes before a Guest Account expires before an SMS is sent.
5. To enable an Email Notification before Expiry, place a check in the Enable box and specify how many minutes before a Guest Account expires before an Email is sent.
6. From the drop down menu select the Language Template you wish to use (Only used for login notifications)
7. Click on Save to continue.

Edit Device Restrictions

Admin can configure the User Profile to place Device Restrictions when a User logs in.

1. From the FortiConnect administration interface, go to Network Access Policy --> Authorization Profiles and click on the Device Restrictions tab as shown below.

Authorization Profiles: Auth Profile One

RADIUS Attributes Locations Notification Settings **Device Restrictions** Auto MAC Registration

Allow Login with: different devices
Leave blank for unlimited

Restrict login with device to: account(s) within 0 Days ▾
Leave blank for unlimited

Save Cancel

2. To allow login with different devices, enter the number of different devices you wish to allow in the Allow to Login with field.
3. To restrict login with a device to a certain amount of accounts within a specific time period, enter the number of accounts in the Restrict login with device to field, then use the field and drop down menu to select the amount of years, days, hours or minutes.
4. Click Save once complete.

Edit Auto MAC Registration

Admin can enable this setting to register MAC addresses, so that when a device is used to login it is remembered on the network.

1. From the FortiConnect administration interface, go to Network Access Policy --> Authorization Profiles and click on the Auto MAC Registration tab as shown below.

Authorization Profiles: Auth Profile One

RADIUS Attributes Locations Notification Settings Device Restrictions **Auto MAC Registration**

! If enabled, a device account is automatically created for a user's device when they login via a portal. Automatic device registration is subject to the limit set in [Policy Settings > Account Groups](#)

Enable: ☐

Account Group: Default Account Group

Usage Profile: Unlimited To define Usage Profiles go to Policy Settings -> Usage Profiles

Save Cancel

If this is enabled, a device account is automatically created for a Users device when they login via a portal. Automatic device registration is subject to the limit set in Policy Settings --> Account Groups

2. To enable Auto MAC Registration place a check in the Enable check box.
3. From the Account Group drop down menu, select the Account Group used to create the device account.
4. From the Usage Profile drop down menu, select the Usage Profile used to create the device account.
5. Click on Save once complete.

Edit Auto MAC Registration

Configuring User Policies

Organizations commonly have policies in place for creating accounts for their internal users and systems, such as the format or length of the username and/or complexity of password. FortiConnect allows you to configure username and password creation policies to match your organization's policy or to create a policy specific to User's accounts.

Usage Profiles allow you to provide different levels of access to different User accounts (for example, to assign different RADIUS attributes, or to only allow access to guests from certain IP address ranges).

This chapter describes the following:

- Setting Username Policy
- Setting Password Policy
- Setting Guest Details Policy
- Configuring Usage Profiles
- Adding Account Groups
- Currency Denomination for Access Codes

Setting Username Policy

The Username Policy determines how to create user names for all accounts.

1. From the administration interface, select Policy Settings > Guest Usernames as shown below and click in the Standard Accounts tab.

2. Username Prefix - All generated usernames will be prefixed with any text/number entered.
3. Choose one of the username policy options for creating the user name for your user accounts:
 - Username Policy 1 - Email address as username

Use the users email address as the username. If an overlapping account with the same email address exists, a random number is added to the end of the email address to make the username unique. Overlapping accounts are accounts that have the same email address and are valid for an overlapping period of time.

With the Create Username With Case option, you can determine the case of the username created by the sponsor:

- **Case entered by sponsor**—The username remains in the same case set by the sponsor.
 - **UPPERCASE**—The username is forced into uppercase after being set by the sponsor.
 - **lowercase**—The username is forced into lowercase after being set by the sponsor.
-
- Username Policy 2 - Create username based on first and last names

Create a username based on combining the first name and last name of the User. You can set a Minimum username length for this username from 1 to 20 characters (default is 8). Usernames shorter than the minimum length are padded up to the minimum specified length with a random number.

With the Create Username With Case option, you can determine the case of the username created by the sponsor:

- **Case entered by sponsor**—The username remains in the same case set by the sponsor.
- **UPPERCASE**—The username is forced into uppercase after being set by the sponsor.
- **lowercase**—The username is forced into lowercase after being set by the sponsor.

- Username Policy 3 - Create random username

Create a username based upon a random mixture of Alphabetic, Numeric or Other characters. Insert the characters to be included in the randomly generated Username, and select and the number to use from each set of characters.

Note: The total length of the username is determined by the total number of characters included.



Sponsor specified username

☒ Sponsor specified username

Minimum username length: 5 ▼

Set Policy Cancel

- Username Policy 4 - Sponsor Specified username

Sponsors can create a username at account creation, click on the dropdown menu and select the minimum username length the sponsor must use.

4. When done, click Set Policy to have the username policy take effect.

To set a policy for Random Bulk Account creation click on the Random Accounts Tab as shown below.

Determine your random account creation policy using the fields provided.

Guest Usernames

Standard Accounts **Random Accounts**

These settings control username policy for multiple random account creation

Username Prefix:
All generated usernames will be prefixed with this text

Alphabetic characters to include:
abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ

Number to include:

Numeric characters to include:
0123456789

Number to include:

Other characters to include:
!\$%^&*()_+=+[]{}~@#-.,<>?

Number to include:

Create username based on the above prefix followed by a sequential number: ☐

Setting Password Policy

The Password Policy determines how to create the password for all User accounts.

1. From the administration interface, select Policy Settings > Guest Passwords as shown below.

Guest Passwords

These settings control password policy for standard account creation

Allow sponsor to change password: ☐

Auto generated password

☒ Auto generated password

Password case: Mixed

Alphabetic characters to include:
abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ

Number to include: 6

Numeric characters to include:
0123456789

Number to include: 2

Other characters to include:
!\$^*()_ = + [] { } ; : @ # ~ , > ?

Number to include: 0

Sponsor specified password

☐ Sponsor specified password

Minimum password length: 5

Set Policy Cancel

2. Check the Allow sponsor to change password box if you wish to allow sponsors to do this.
3. From the Password case drop down menu select whether the password that is generated will have a mixed, lowercase or uppercase character base.
4. In the Alphabetic Characters section, enter the characters to be used in the password and the number to be included.
5. In the Numeric Characters section, enter the numerals to be used in the password and the number to be included.
6. In the Other Characters section, enter the special characters to be used in the password and the number to be included.
7. You may also allow the sponsor to specify the password. If you wish to select this option, place a check in the Sponsor specified password section and using the drop down menu choose the minimum number of characters a sponsor should use when creating a password for the User.

Note: For passwords, use only the following characters for the “Other Characters” field: !\$^&*()-_+=[]{};:@#~,>?

8. Click the Set Policy button to save the settings.

Note: The total length of the password is determined by the total number of characters included. You can choose between 0 and 20 characters per type (alphabetic, numeric, or other).

Setting Account Details Policy

The Guest Details policy determines the data the sponsor needs to enter to create a User account.

1. From the administration interface, select Policy Settings > Guest Details as shown below.

The screenshot shows the 'Guest Details' configuration page. It has a blue header bar with the title 'Guest Details'. Below the header, there are two sections: 'Standard Fields' and 'Additional Fields'. In the 'Standard Fields' section, there are five rows, each with a label and a dropdown menu: 'First Name: Required', 'Last Name: Required', 'Company: Required', 'Email: Required', and 'Mobile: Optional'. A note below the 'Email' field states: 'This cannot be changed as email address is being used as the username in Guest Usernames settings'. The 'Additional Fields' section has a heading 'Additional Fields' followed by a note: 'The text for additional fields is defined in the [Language Templates](#) section'. Below this note are five rows, each with a label and a dropdown menu: 'Option 1: Unused', 'Option 2: Unused', 'Option 3: Unused', 'Option 4: Unused', and 'Option 5: Unused'. At the bottom of the form are two buttons: 'Save' and 'Cancel'.

2. You can specify one of three settings for each requirement:
 - **Required**—If a field is set to required it is displayed on the Create Guest Account page and it is mandatory for the sponsor to complete.
 - **Optional**—If a field is set to optional it is displayed on the Create Guest Account page. However

the sponsor can choose not to complete the field.

- **Unused**—If a field is set to unused then it is not displayed on the Create Guest Account page and no value is required.

3. Click the Save Settings button to save the guest details policy.

Note: There are five Additional Fields that you can use to add any additional information that you require sponsors to fill out when creating guest accounts. These are described on the Guest Details page as Option 1 through Option 5. If you want to use these fields, Fortinet recommends customizing the text that is shown to the sponsor by editing the templates as described in User Interface Templates.

Configuring Usage Profiles

Usage Profiles provide a way to give levels of time access to different User accounts, or, also a level of Data Usage. For example, you can assign a usage profile that allows access during a working week day and not on a weekend.

Once Usage profiles are created, you must change the sponsor user group to allow sponsors in that group to be able to provision accounts to the appropriate usage profiles created.







Adding Usage Profiles

You can add a new usage profile using the following steps.

1. From the administration interface, select Policy Settings > Usage Profiles as shown below.

Adding Usage Profiles

Usage Profiles

Name	Description	Account Type	Timezone	
12 Hours	12 hours usage from first login	From First Login	America/Los_Angeles	
1 Hour	1 hour usage from first login	From First Login	America/Los_Angeles	
24 Hours	24 hours usage from first login	From First Login	America/Los_Angeles	
6 Hours	6 hours usage from first login	From First Login	America/Los_Angeles	
default	Default time profile	Start End	America/Los_Angeles	
Unlimited	Unlimited time profile	Unlimited	America/Los_Angeles	

Add

- Click the Add button to add a new Usage Profile.
- From the Usage Profile page as shown below, Click on the Time Usage tab and type the Name and Description of the new time profile.

4. From the Timezone dropdown menu, specify the timezone for which any Account Restrictions will apply.
5. From the Account Type dropdown menu, you can choose one of the predefined options.
 - Start End—Allows sponsors to define start and end times for account durations.
 - From First Login—Allows sponsors to define a length of time for User access from their first login.
 - From Creation - Allows sponsors to define a length of time for User access from the moment of account creation.
 - Time Used—Allows sponsors to create a time period during which the User can login. For example, account can be valid for 2 hours and usable for any time within 24 hours from first login.
 - Unlimited - Unlimited time profiles
6. Expire if inactive for - Allows the admin to specify the time period after which an account with this usage profile should be considered inactive.

Note: When creating an account type of Time Used, you may also repeat the time used as many times as you require by entering an amount into the Repeat Field, as shown below

Adding Usage Profiles

•

The screenshot shows the 'Usage Profile' configuration page with the 'Time Usage' tab selected. The page has a blue header bar with the text 'Usage Profile:'. Below the header, there are three tabs: 'Time Usage' (selected), 'Time Restrictions', and 'Data Usage'. The 'Time Usage' tab contains the following fields:

- Name:
- Description:
- Time zone:
- Account Type:
- Duration: Hours Within Hours
- Repeat: more times (ends after 0 hours)
- Expire if inactive for: Days

Below the fields, there are two buttons: 'Save' and 'Cancel'. A small note at the bottom of the 'Expire if inactive for' field states: '0 = never expire'.

7. Once you have selected your account type, click on Save.
8. Next, click on the Time Restrictions tab as shown below.

The screenshot shows the 'Usage Profile: test' configuration page with the 'Time Restrictions' tab selected. The page has a blue header bar with the text 'Usage Profile: test'. Below the header, there are three tabs: 'Time Usage', 'Time Restrictions' (selected), and 'Data Usage'. The 'Time Restrictions' tab contains the following content:

Guests cannot login or will be logged out during these periods

No current restrictions for this profile

<input type="text" value="Monday"/>	<input type="text" value="00"/>	<input type="text" value="00"/>	<input type="text" value="23"/>	<input type="text" value="59"/>	<input type="button" value="Add"/>
-------------------------------------	---------------------------------	---------------------------------	---------------------------------	---------------------------------	------------------------------------

9. Once a Time Profile is created, you can implement Account Restrictions in the Time Restrictions section. Use the dropdown menus to select the days and time you wish to restrict guest access to and from. Once a time criteria is complete, click Add, then create the next restriction.
10. Depending on the Account Type selected, enter the duration in the following fields:
 - Start End—Allows sponsors to define start and end times for account durations; therefore, no duration is necessary.

- **From First Login**—Allows sponsors to define a length of time for User access from their first login. Duration in days is required.
- **From Creation** - Allows sponsors to define a length of time for User access from the moment of account creation.
- **Time Used**—Allows sponsors to create a time period during which the User can login. For example account can be valid for 2 hours and usable for any time within 24 hours from first login. You need to specify how long the sponsor can allocate a User account for, and the time frame in which it must end.
- **Unlimited** - No action necessary.
- Click the Save button to save.

11. Next Click on the Data Usage tab as shown below.

Usage Profile: test

Time Usage | Time Restrictions | **Data Usage**

Accounts will be expired when the first limit is reached

Data Up: KB
0 = unlimited

Data Down: KB
0 = unlimited

Total Up & Down: KB
0 = unlimited

12. You can also add Data Usage restriction to your Usage Profiles.

13. From the drop down menus, determine whether to apply the following -

- **Data Up** - Apply a Data Usage up restriction to your profile, use the drop down menu to determine whether it be in KB, MB or GB.
- **Data Down** - Apply a Data Usage down restriction to your profile, use the drop down menu to determine whether it be in KB, MB or GB.
- **Total Up & Down** - Apply a Total Data Usage restriction to your profile, use the drop down menu to determine whether it be in KB, MB or GB.








14. Click on Save once complete.

Editing Usage Profiles

The following steps describe how to edit Usage Profiles.

1. From the administration interface, select Policy Settings > Usage Profiles from the left hand menu.

Usage Profiles

Name	Description	Account Type	Timezone	
12 Hours	12 hours usage from first login	From First Login	America/Los_Angeles	
1 Hour	1 hour usage from first login	From First Login	America/Los_Angeles	
24 Hours	24 hours usage from first login	From First Login	America/Los_Angeles	
6 Hours	6 hours usage from first login	From First Login	America/Los_Angeles	
default	Default time profile	Start End	America/Los_Angeles	
test	test	Start End	America/Los_Angeles	
Unlimited	Unlimited time profile	Unlimited	America/Los_Angeles	

Add








2. Select the usage profile you wish to edit and click the underlined name of that profile as shown above.
3. Repeat the steps in the Adding a Usage Profile section above to make the necessary amendments.

Deleting Time Profiles

The following steps describe how to delete Usage Profiles.

1. From the administration interface, select Policy Settings > Usage Profiles from the left hand menu.

Usage Profiles

Name	Description	Account Type	Timezone	
12 Hours	12 hours usage from first login	From First Login	America/Los_Angeles	
1 Hour	1 hour usage from first login	From First Login	America/Los_Angeles	
24 Hours	24 hours usage from first login	From First Login	America/Los_Angeles	
6 Hours	6 hours usage from first login	From First Login	America/Los_Angeles	
default	Default time profile	Start End	America/Los_Angeles	
test	test	Start End	America/Los_Angeles	
Unlimited	Unlimited time profile	Unlimited	America/Los_Angeles	

Add

2. From the Usage Profiles page as shown above, choose the profile you wish to delete and click the dustbin icon.
3. Confirm the deletion when prompted.

Account Groups

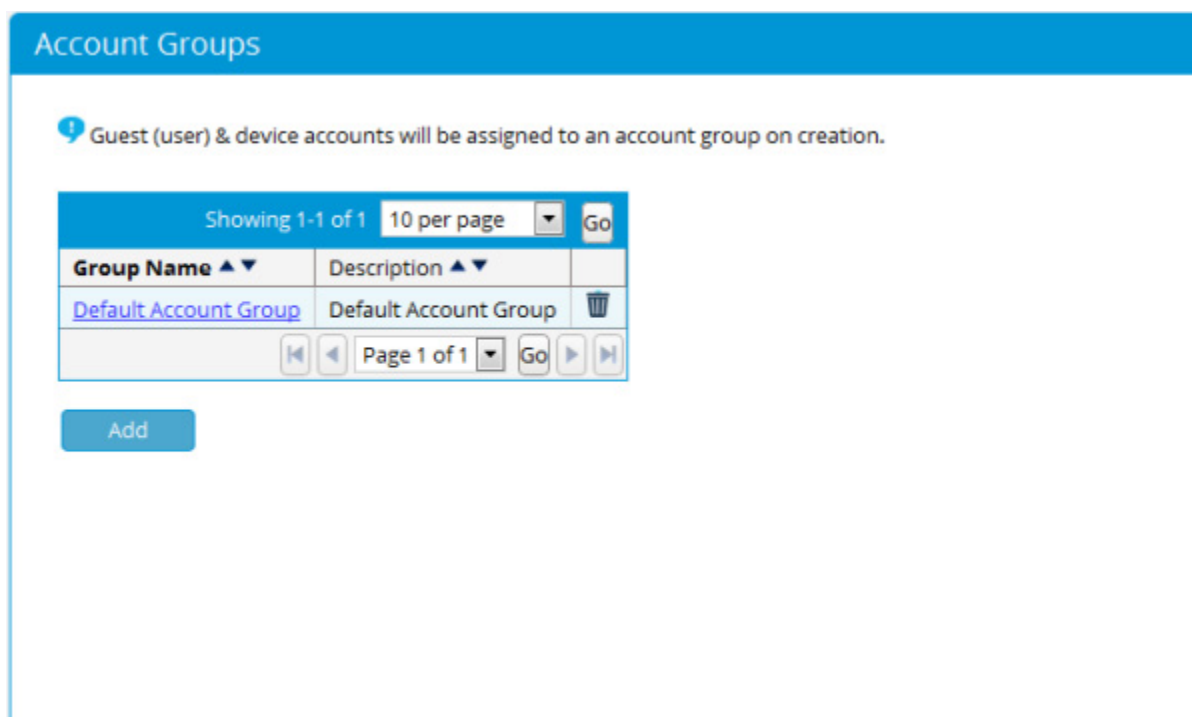
Account Groups are used to group User & device accounts and are assigned at the point of account creation. If no additional account groups are created, User & device accounts will be assigned to the default account group.

In previous versions of Identity Manager (now FortiConnect), User and device accounts could be assigned an authorization profile at creation. This is no longer the case and instead we assign an account group to the User or device account.

An Authorization Profile will be assigned via the Authorization Policy which may reference an Account Group as part of its mapping criteria.

Adding Account Groups

From the FortiConnect Administration Interface go to Policy Settings --> Account Groups as shown below.



1. By default User and device accounts will be assigned to the Default Account Group, to add another group click on the Add button.

Add Account Group

Details

Name:

Description:

Authentication Settings

Maximum Concurrent Connections:
0 = unlimited

Maximum Failed Authentications:
0 = unlimited

Allow Password Change: ☐

Require Password Change: ☐

Guest Portal Device Registration Limit

Maximum Number Of Different Devices:
0 = unlimited

2. Edit the fields as required -


- Name - Enter the name of your group
- Description - Enter the group description
- Maximum Concurrent Connections - Enter the maximum amount of concurrent connections allowed
- Maximum Failed Authentications - Enter the maximum amount of failed authentications allowed
- Allow Password Change - Check box to allow passwords to be changed
- Require Password Change - Check box to require passwords be changed (applies to accounts create on FortiConnect only)
- Maximum Number Of Different Devices - Specify the maximum number of different devices a user can register

3. Click on Save once complete

Editing Account Groups

From the FortiConnect Administration Interface go to Policy Settings --> Account Groups as shown below.

Account Groups

 Guest (user) & device accounts will be assigned to an account group on creation.

Showing 1-1 of 1
10 per page ▾
Go

Group Name ▲ ▾	Description ▲ ▾	
Default Account Group	Default Account Group	🗑

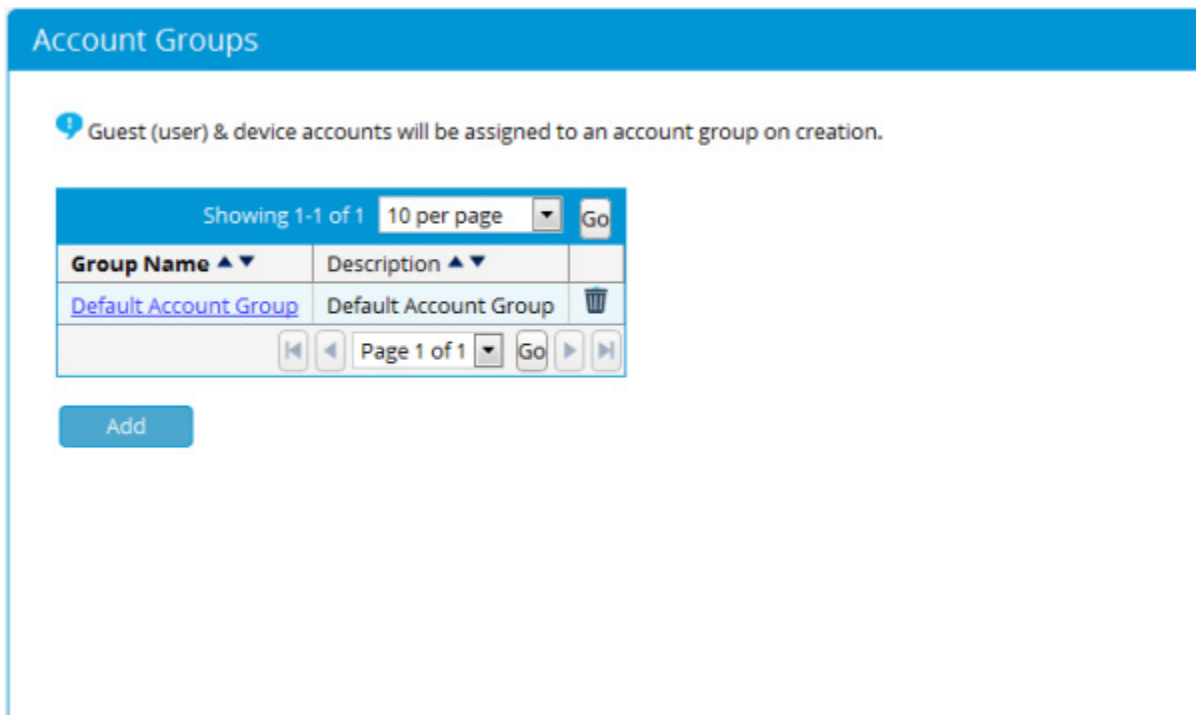
⏪ ⏴
Page 1 of 1 ▾
Go ⏵ ⏩

Add

1. Click on the Group Name of the group you wish to edit.
2. Edit the fields as required -
 - Name - Enter the name of your group
 - Description - Enter the group description
 - Maximum Concurrent Connections - Enter the maximum amount of concurrent connections allowed
 - Maximum Failed Authentications - Enter the maximum amount of failed authentications allowed
 - Allow Password Change - Check box to allow passwords to be changed
 - Require Password Change - Check box to require passwords be changed
 - Maximum Number Of Different Devices - Specify the maximum number of different devices allowed to be registered.
3. Click on Save once complete.

Deleting Account Groups

From the FortiConnect Administration Interface go to Policy Settings --> Account Groups as shown below.



1. Click on the Bin Icon of the group you wish to delete.
2. Click on Ok to delete.

Currency Denomination for Access Codes

In some environments, credit card based purchases are not widely used, and there is a larger interest in using access codes with currency denominations attached to them.

FortiConnect can set a Currency Denomination which will allow a sponsor to create multiple numbers of random User accounts assigned to a time profile, and then export them to a CSV file to print and create an offline coupon or scratch card to distribute to the User.

1. From the FortiConnect Administration Interface go to Sponsor Portal --> Currency as shown below.

Currency Settings

Sponsor Portal Currency:

Save

2. From the dropdown menu, select the Sponsor Portal Currency you wish to set.

Configuring Sponsor User Groups

Sponsor user groups are the method by which you assign permissions to the sponsors. You can set role-based permissions for sponsors to allow or restrict access to different functions, such as creating accounts, modifying accounts, generating reports, and sending account details to Users by email or SMS.

Once you have created a User group, create mapping rules to map the sponsor to a group based upon information returned from the authentication server such as Active Directory Group, LDAP Group membership, or RADIUS Class attribute.

TIP - By default, all Users are assigned to the DEFAULT group. If you only want to have a single classification of sponsors, you can edit the DEFAULT group.

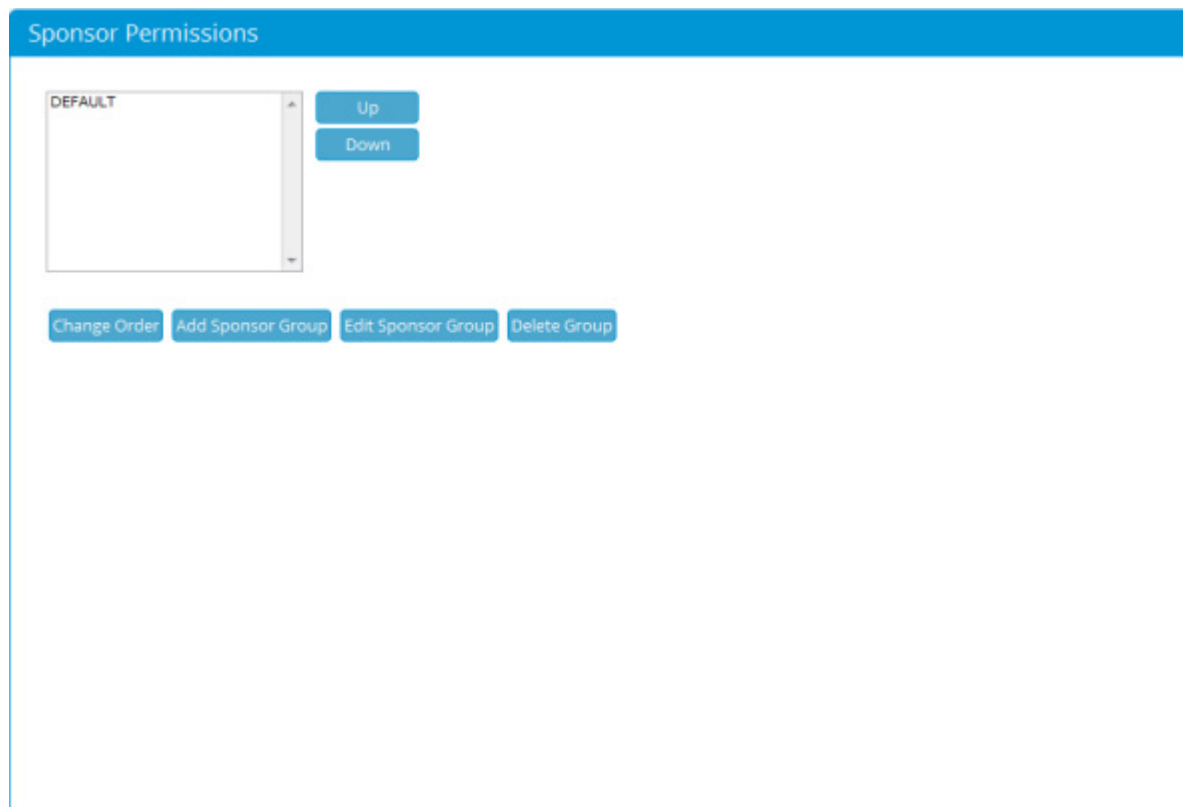
This chapter describes the following:

- Adding Sponsor User Groups
- Editing Sponsor User Groups
- Deleting User Groups
- Specifying the Order of Sponsor User Groups
- Mapping to Active Directory Groups
- Mapping to LDAP Groups
- Mapping to RADIUS Groups
- Assigning User Account Groups
- Assigning Usage Profiles

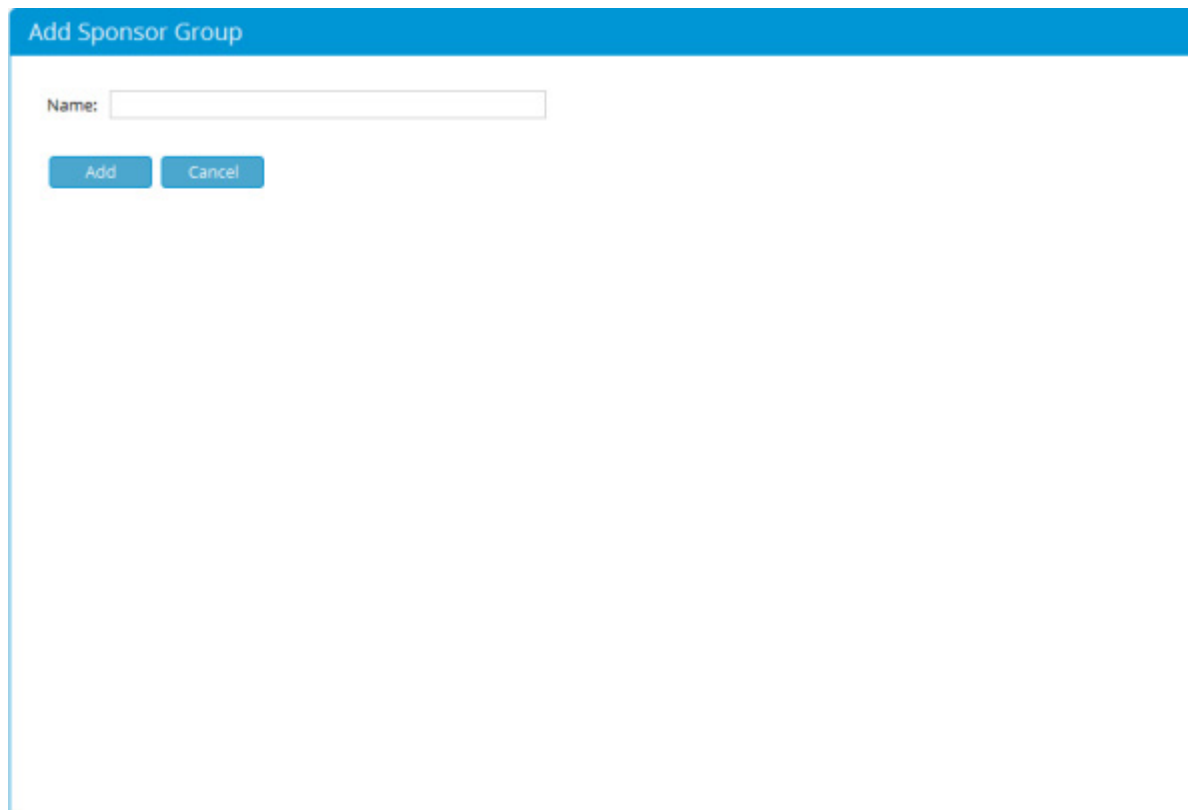
Adding Sponsor User Groups

You can create a new sponsor user group using the following steps.

1. From the administration interface, select Sponsor Portal > Sponsor Permissions as shown below.



2. Click the Add Sponsor Group button to add a new user group.
3. From the Add a New Sponsor Group page as shown below, type the name for a new user group in the Sponsor Group Name field.



Add Sponsor Group

Name:

Add Cancel

4. Click the Add Sponsor Group button to add a user group. You can now edit the settings for the new user group as detailed below.
5. Edit and set the permissions for the new User Group as follows:
 - Allow Login—Select Yes to allow sponsors in this group to access FortiConnect.
 - Create Guest Accounts—Select Yes to allow sponsors to create accounts.
 - Create Multiple Guest Accounts—Select Yes to allow sponsors to be able to create multiple accounts at a time by pasting in the details.
 - Create Random Guest Accounts—Select Yes to allow sponsors to be able to create multiple random accounts without initially capturing the Users details.
 - Email Manager on Guest Account Creation - Automatically email a sponsors manager when an account has been created. (LDAP setup only)
 - Create Device Accounts - Select Yes to allow sponsors to be able to create device accounts.
 - Create Multiple Device Accounts - Select Yes to allow sponsors to be able to create multiple accounts at a time by filling in the appropriate form or importing a csv in the details.
 - Email Manager on Device Account Creation - Automatically email a sponsor's manager when a device account has been created. (LDAP setup only)
 - Send Email—Select Yes to allow sponsors to send account details via email from FortiConnect to the user.

- **Send SMS**—Select Yes to allow sponsors to send account details via SMS from the FortiConnect to the User.
- **View Guest Account Password**—Select Yes to allow sponsors to view the password that has been created for the User.
- **Print Account Details**—Select Yes to allow sponsors to print out the account details.

Note: Select No, if you want to disable any of the above permissions.

- **Reset Account Password** - Choose one of the following options to allow a sponsor to reset account passwords.
 - No**—Sponsors are not allowed to reset any account passwords.
 - Own Account**—Sponsors are allowed to reset only the account passwords they created.
 - Group Accounts**—Sponsors are allowed to reset account passwords created by anyone in the same sponsor user group.
 - All Accounts**—Sponsors are allowed to reset any account passwords in any User accounts
- **Suspend Account**—Choose one of the following options for suspending accounts:
 - No**—Sponsors are not allowed to suspend any User accounts.
 - Own Account**—Sponsors are allowed to suspend only the User accounts they created.
 - Group Accounts**—Sponsors are allowed to suspend User accounts created by anyone in the same sponsor user group.
 - All Accounts**—Sponsors are allowed to suspend any User accounts.
- **Edit Account**—Choose one of the following permissions for editing the end date/time on User accounts:
 - No**—Sponsors are not allowed to edit any guest accounts.
 - Own Account**—Sponsors are allowed to edit only the User accounts they created.
 - Group Accounts**—Sponsors are allowed to edit User accounts created by anyone in the same sponsor user group.
 - All Accounts**—Sponsors are allowed to edit any User accounts.
- **UnSuspend Account**—Choose one of the following options for suspending accounts:
 - No**—Sponsors are not allowed to unsuspend any User accounts.
 - Own Account**—Sponsors are allowed to unsuspend only the User accounts they created.
 - Group Accounts**—Sponsors are allowed to unsuspend User accounts created by anyone in the same sponsor user group.
 - All Accounts**—Sponsors are allowed to unsuspend any User accounts.
- **Reactivate Expired Account** :
 - No**—Sponsors are not allowed to reactivate any accounts.
 - Own Account**—Sponsors are allowed to reactivate only the accounts they created.
 - Group Accounts**—Sponsors are allowed to reactivate accounts created by anyone in the same sponsor user group.
 - All Accounts**—Sponsors are allowed to reactivate User accounts.

- **Report & Manage Accounts**—Choose one of the following permissions for viewing reporting details for full reporting. See Reporting on Users for additional details.
 - No**—Sponsors are not allowed to view reporting details on any User accounts.
 - Own Account**—Sponsors are allowed to view reporting details for only the User accounts they created.
 - Group Accounts**—Sponsors are allowed to view active User accounts created by anyone in the same sponsor user group.
 - All Accounts**—Sponsors are allowed to view reporting details on any active User accounts.
- **Guest Accounts Detailed Reports-Accounting Log** —Choose one of the following permissions for running a full report on accounting logs:
 - No**—Sponsors are not allowed to run accounting log reporting on any User accounts.
 - Own Account**—Sponsors are allowed to run full accounting log reporting for only the User accounts they created.
 - Group Accounts**—Sponsors are allowed to run full reporting on User accounts created by anyone in the same sponsor user group.
 - All Accounts**—Sponsors are allowed to run full accounting log reporting on any active User accounts.
- **Guest Accounts Detailed Reports - Audit Log**—Choose one of the following permissions for running a full report on audit logs:
 - No**—Sponsors are not allowed to run an audit log report on logs on any accounts. **Own Account**—Sponsors are allowed to run an audit log report on logs for only the User accounts they created.
 - Group Accounts**—Sponsors are allowed to run an audit log report on logs for User accounts created by anyone in the same sponsor user group.
 - All Accounts**—Sponsors are allowed to a run an audit log report on logs on any active User accounts.
- **Guest Accounts Detailed Reports - Activity Log**—Choose one of the following permissions for running a full report on activity logs.
 - No**—Sponsors are not allowed to run detailed reports on activity logs on any User accounts.
 - Own Account**—Sponsors are allowed to run detailed reports on activity logs for only the User accounts they created.
 - Group Accounts**—Sponsors are allowed to run a detailed report on activity logs for User accounts created by anyone in the same sponsor user group.
 - All Accounts**—Sponsors are allowed to run detailed reports on activity logs on any active User accounts.
- **View Guest Payments Report** - Choose one of the following permissions for viewing User Payments
 - No** - Sponsors are not allowed to run detailed reports on User Payments.
 - Own Account** - Sponsors are allowed to run detailed reports on User Payments for accounts only they have created.
 - Group Accounts** - Sponsors are allowed to run reports on User Payments for only accounts created by anyone in the same sponsor group.
 - All Accounts** - Sponsors are allowed to run reports on User Payments on any active User account.
- **Charge/Refund Paid User Accounts** - Choose one of the following permissions for allowing sponsors to charge or refund paid User accounts.
 - No** - Sponsors are not allowed to charge or refund paid User accounts.
 - Own Account** - Sponsors are allowed to charge or refund paid User accounts on accounts only they have created.

Group Accounts - Sponsors are allowed to charge or refund paid User accounts created by anyone in the same sponsor group.

All Accounts - Sponsors are allowed to charge or refund paid User accounts on any active User account.

- **Concurrent User Reports** –Select Yes to allow the sponsors to run the concurrent User reports. If you select No, the sponsors are not allowed to run the reports.
 - **Management Reports**–Select Yes to allow the sponsors to run the management reports. If you select No, the sponsors are not allowed to run the reports.
 - **Create Event Codes** - Select Yes to allow the sponsors to Create Event Codes.
 - **Edit Event Codes** - Choose one of the following permissions for Editing Event Codes
 - No** - Sponsors are not allowed to Edit Event Codes
 - Own Event Codes** - Sponsors can only Edit Event Codes they create.
 - Group Event Codes** - Sponsors can Edit Event Codes within a Group.
 - All Event Codes** - Sponsors can Edit All Event Codes.
 - **Suspend Event Codes** - Choose one of the following permissions for Suspending Event Codes
 - No** - Sponsors are not allowed to Suspend Event Codes.
 - Own Event Codes** - Sponsors can only Suspend Event Codes they create.
 - Group Event Codes** - Sponsors can only Suspend Event Codes in a Group.
 - All Event Codes** - Sponsors can Suspend all Event Codes
 - **Manage Event Codes** - Choose one of the following permissions for Managing Event Codes.
 - No** - Sponsors are not allowed to Manage Event Codes
 - Own Event Codes** - Sponsors can only Manage Event Codes they create.
 - Group Event Codes** - Sponsors can only Manage Event Codes in a Group.
 - All Event Codes** - Sponsors Manage all Event Codes.
 - **Approve Accounts** - Select Yes to allow the sponsors to Approve Accounts.
 - **Account start time within** - Select the amount of days the account should start in. Specify the time interval in days, hours, or minutes.
 - **Maximum duration of User account**—This specifies the maximum duration for which the sponsor can configure an account. Specify the duration in days, hours, or minutes.
 - **Maximum duration of device account** - This specifies the maximum duration for which the sponsor can configure a device account. Specify the duration in days, hours, or minutes.
 - **Maximum duration restriction calculated from** - From the drop down menu select whether restrictions apply from current time or from start time.
 - **User Account limit** - Specify the maximum number of allowed active User accounts a sponsor from this group can have at any given time, 0 for unlimited.
 - **Device Account limit** - Specify the maximum number of allowed active device accounts a sponsor from this group can have at any given time, 0 for unlimited.
6. Click the Save button to add the group with the permissions specified.

Note: Until you click the Save button, the group is not created.

7. Execute one of the following set of instructions to correctly map sponsor users to your group based upon group information from the authentication server:
 - Mapping to Active Directory Groups
 - Mapping to LDAP Groups
 - Mapping to RADIUS Groups

Editing Sponsor User Groups

The following steps describe how to edit sponsor user groups.

1. From the administration interface, select Sponsor Portal > Sponsor Permissions from the left hand menu.
2. Select and highlight the group you wish to edit, then click Edit Sponsor Group button to get the screen as shown below

Sponsor Permissions: Sponsor Group One	
Group Permissions Group Mappings Guest Account Groups Guest Usage Profiles Device Account Groups Device Usage Profiles Sponsor Preferences	
Allow Login:	No
Create Guest Accounts:	No
Create Multiple Guest Accounts:	No
Create Random Guest Accounts:	No
Set Random Account Price:	No
Email Manager on Guest Account Creation:	No
Create Device Accounts:	No
Create Multiple Device Accounts:	No
Email Manager on Device Account Creation:	No
Send Email:	No
Send SMS:	No
View Account Password:	No
Print Account Details:	No
Reset Account Password:	No
Suspend Account:	No
Edit Account:	No

3. Edit and set the permissions by following the steps as was followed in the Create Sponsor Groups Section

Deleting User Groups

1. From the administration interface, select Sponsor Portal > Sponsor Permissions from the left hand menu.



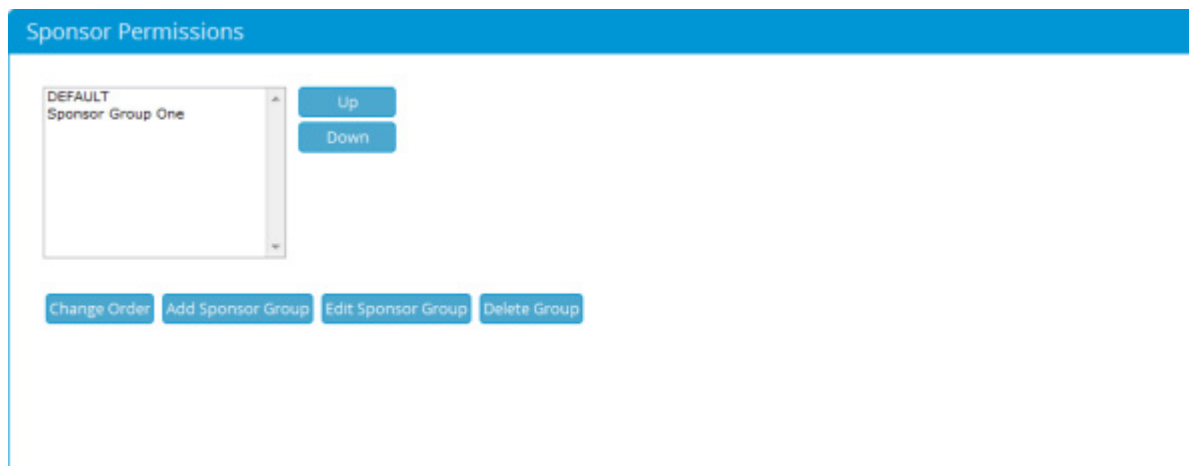
2. Select and highlight the group you wish to delete and click the Delete Group button as shown above.
3. Confirm deletion at the prompt.

Note: If any Local Users are part of this group, you must delete the user before deleting the user group. Alternatively, you can move Local Users to another group to “empty” the user group before deleting it.

Specifying the Order of Sponsor User Groups

When a sponsor logs in to the FortiConnect, the system checks each group in turn to see if the sponsor should be given the privileges of that group. The groups are processed in the order in which they appear in the Sponsor User Groups list box. If a user does not match a user group, they are given the privileges of the DEFAULT group.

1. From the administration interface, select Sponsor Portal> Sponsor Permissions from the left hand menu.



2. Select the group you wish to order. Each group can be ordered by clicking the up or down arrow icon button until the group is in position as shown in above.
3. Repeat for all groups until they appear in the required order.
4. Click the Change Order button to save the order.

Mapping to Groups

Mapping to Active Directory Groups

If a sponsor authenticates to the FortiConnect using Active Directory authentication, the FortiConnect can map the sponsors into a user group using their membership in Active Directory groups.

Note: FortiConnect does support recursive group lookups.

If you have configured AD authentication (as described in Configuring Active Directory (AD) Authentication), then the FortiConnect automatically retrieves a list of all the groups configured within all the AD servers.

Selecting an Active Directory Group from the dropdown provides all sponsor users in this AD group the permissions assigned to this Sponsor Group.

Mapping to LDAP Groups

If a sponsor authenticates to the FortiConnect using LDAP authentication, the FortiConnect can map the sponsor into a user group by their membership of LDAP groups.

Note: FortiConnect does support recursive group lookups.

Based on the settings of the LDAP server that you authenticate against, the FortiConnect uses one of the following methods for mapping the sponsor using group information.

Mapping to RADIUS Groups

If a sponsor authenticates to the FortiConnect using RADIUS authentication, the FortiConnect can map the sponsor into a user group by using information returned to the FortiConnect in the authentication request.

The information must be placed into the class attribute on the RADIUS server.

Mapping the Groups

1. From the administration interface, select Sponsor Portal > Sponsor Permissions from the left hand menu.
2. Select and highlight the group you wish to edit, then click Edit Sponsor Group button.
3. Click on the Group Mappings tab.
4. Using the rule underneath the Sponsor Group table, shown below, you can create new rules using the Sponsor Authentication methods you have added.

Sponsor Permissions: Sponsor Group One

Group Permissions **Group Mappings** Guest Account Groups Guest Usage Profiles Device Account Groups Device Usage Profiles Sponsor Preferences

The Sponsor will be in this group if they match any of the following rules:

10 per page Go

Server ▲▼	Rule ▲▼
No Group Mappings defined	

If the Sponsor is authenticated against server 10.10.1.2 check class attribute equals Add Rule

- From the drop down menu, select the desired server you wish to create a rule for.
 - Then select whether the group class names equals or contains the term from the drop down menu.
 - Enter the term the mapping should be based on into the empty field and click Add Rule.
5. The rule is then added to the table.
 6. To remove a rule click on the bin icon to the right of the rule.

Note: By default, Active Directory only returns a maximum of 1000 groups in response to a FortiConnect search. If you have more than 1000 groups and have not increased the LDAP search size, it is possible that the group you want to match does not appear. In this situation, you can manually enter the group name in the Active Directory Group combo box.

Assigning Guest Account Groups

Guest Groups allow a sponsor to assign different levels of access to a User account. You can choose which sponsor user groups are allowed to assign certain profiles to Users.

By default, a sponsor user group has the ability to assign Users to the default profile. The administrator can choose the additional groups the sponsor can assign, or can remove the default profile from the user group.

Each sponsor user group must have the ability to assign Users to at least one role.

If only one role is selected for the user group, the sponsor cannot have the option to select roles. If there is more than one role, sponsors get a dropdown menu to select the role to be assigned to the account during the account creation.

1. From the administration interface, select **Sponsor Portal > Sponsor Permissions** from the left hand menu.
2. Select and highlight the group you wish to edit, then click **Edit Sponsor Group** button.
3. Click the **Guest Account Groups** tab to bring up the Available Account groups as shown below.

Sponsor Permissions: Sponsor Group One

Group Permissions | Group Mappings | **Guest Account Groups** | Guest Usage Profiles | Device Account Groups | Device Usage Profiles | Sponsor Preferences

Selected Account Groups are the groups that a sponsor can select when creating guest accounts.

Available Account Groups

Selected Account Groups

Default Account Group

Save Cancel

4. The roles that the sponsor has permission to assign are displayed in the Selected Account Groups list. Move the roles between the Available Account Groups and Selected Account Groups lists using the arrow buttons.
5. Click the Save button to assign the permission to create Users in the specified profiles to the sponsor user group.

Assigning Guest Usage Profiles

Usage Profiles allow a sponsor to assign different levels of access usage to a User account. You can choose the sponsor user groups that are allowed to assign certain Usage Profiles to guests.

By default, a user group has the ability to assign guests to the default usage profile. The administrator can choose which additional usage profiles the sponsor can be assigned, or can remove the default usage profile from the user group.

Each user group must have the ability to assign Users in at least one usage profile.

If a user group has only one usage profile selected, the sponsor does not view an option to select the usage profile. If they have the ability to choose more than one usage profile, they can view a dropdown menu from which they can choose the usage profile to be assigned to the account during the account creation.

Refer to [Configuring Usage Profiles](#) for additional details on usage profiles.

1. From the administration interface, select **Sponsor Portal > Sponsor Permissions** from the left hand menu.
2. Select and highlight the group you wish to edit, then click **Edit Sponsor Group** button.
3. Click the **Guest Usage Profiles** tab to bring up the Edit Usage Profiles as shown below.

Sponsor Permissions: Sponsor Group One

Group Permissions | Group Mappings | Guest Account Groups | **Guest Usage Profiles** | Device Account Groups | Device Usage Profiles | Sponsor Preferences

Selected Profiles are the Usage Profiles a sponsor in this group can select when creating guest accounts.

Available Profiles

- Unlimited
- 6 Hours
- 24 Hours
- test
- 1 Hour
- 12 Hours

Selected Profiles

- default

<< >>

Save Cancel

4. The profiles that the sponsor user group has permission to assign are displayed in the **Available Profiles** list. Move the roles between the **Available Profiles** and **Selected Profiles** lists using the arrow buttons.
5. Click the **Save** button to assign the permission to create Users in the usage profiles to the sponsor user group.

Assigning Device Account Groups

Device Account Groups allow a sponsor to assign different levels of access to a device account. You can choose which sponsor user profiles are allowed to assign certain Account Groups to device accounts.

By default, a sponsor user group has the ability to assign device accounts to the default role. The administrator can choose the additional groups the sponsor can assign, or can remove the default role from the user group.

Each sponsor user group must have the ability to assign Users to at least one role.

If only one group is selected for the user group, the sponsor will not have the option to select groups. If there is more than one group, sponsors get a dropdown menu to select the role to be assigned to the account during the account creation.

1. From the administration interface, select **Sponsor Portal > Sponsor Permissions** from the left hand menu.
2. Select and highlight the group you wish to edit, then click **Edit Sponsor Group** button.
3. Click the **Device Account Groups** tab to bring up the Edit Authorization Profiles as shown below.

Sponsor Permissions: Sponsor Group One

Group Permissions | Group Mappings | Guest Account Groups | Guest Usage Profiles | **Device Account Groups** | Device Usage Profiles | Sponsor Preferences

Selected Account Groups are the groups that a sponsor can select when creating device accounts.

Available Account Groups

Selected Account Groups

Default Account Group

<< >>

Save Cancel

4. The groups that the sponsor user group has permission to assign are displayed in the Selected Account Groups list. Move the groups between the Available Account Groups and Selected Account Groups lists using the arrow buttons.
5. Click the Save button to assign the permission to create Users in the specified groups to the sponsor user group.

Assigning Device Usage Profiles

Device Usage Profiles allow a sponsor to assign different levels of access usage to a device account. You can choose the sponsor user groups that are allowed to assign certain Device Usage Profiles to Users.

By default, a user group has the ability to assign Users to the default device usage profile. The administrator can choose which additional usage profiles the sponsor can be assigned, or can remove the default device usage profile from the user group.

Each user group must have the ability to assign Users in at least one device usage profile.

If a user group has only one usage profile selected, the sponsor does not view an option to select the usage profile. If they have the ability to choose more than one usage profile, they can view a dropdown menu from which they can choose the usage profile to be assigned to the account during the account creation.

1. From the administration interface, select Sponsor Portal > Sponsor Permissions from the left hand menu.
2. Select and highlight the group you wish to edit, then click Edit Sponsor Group button.
3. Click the Device Usage Profiles tab to bring up the Edit Usage Profiles as shown below.

1. The usage profiles that the sponsor user group has permission to assign are displayed in the Available Profiles list. Move the roles between the Available Profiles and Selected Profiles lists using the arrow buttons.
2. Click the Save button to assign the permission to create Users in the usage profiles to the sponsor user group.

Sponsor Preferences

Administrators can restrict/disable or enable controls on a sponsors default preferences page. The section below details the default values for these preferences.

1. From the administration interface, select Sponsor Portal > Sponsor Permissions from the left hand menu.
2. Select and highlight the group you wish to edit, then click Edit Sponsor Group button.
3. Click the Sponsor Preferences tab to bring up the Edit Sponsor Settings as shown below.

Sponsor Permissions: Sponsor Group One

Group Permissions | Group Mappings | Guest Account Groups | Guest Usage Profiles | Device Account Groups | Device Usage Profiles | **Sponsor Preferences**

These settings assign default values & enable / disable controls on the Sponsor Interface > My Settings > Preferences page

Language Template

Default Language Template: English (Default) ▼

Allow sponsor to change: Yes ▼

Available Templates

Currently Selected

- Danish
- Hebrew
- Ukrainian
- Finnish
- Spanish
- English (Default)
- Greek
- Czech

Timezone

Default Timezone: America/Los_Angeles ▼

Allow sponsor to change: Yes ▼

Country Code

Default Country Code: +1 ▼

Allow sponsor to change: Yes ▼

Guest Account Groups

4. Language Template -

- Default Template - Choose a template from the drop down menu provided
- Allow Sponsor to change - Choose yes or no from the drop down menu.
- Move any templates you wish to be available to the currently selected list by highlighting the template and clicking the correct arrow.

5. Timezone -

- Default Timezone - Select a default timezone from the drop down menu provided.
- Allow Sponsor to change - Choose yes or no from the drop down menu.

6. Country Code -

- Default Country Code - Select a default country code from the drop down menu provided.
- Allow Sponsor to change - Choose yes or no from the drop down menu.

7. Guest/User Account Group -

- Default Group - Select a default group from the drop down menu provided.
- Allow Sponsor to change - Choose yes or no from the drop down menu.

8. Device Account Group -

- Default Device Group - Select a default device group from the drop down menu provided.

- Allow Sponsor to change - Choose yes or no from the drop down menu.
- 9. Email Address -**
- Enter a check in the Retrieve from LDAP box if this function is required.
 - Allow Sponsor to change - Choose yes or no from the drop down menu.
- 10. Email Confirmation -**
- Default setting - Select a default setting from the drop down menu provided
 - Allow Sponsor to change - Choose yes or no from the drop down menu.
- 11. Login Page -**
- Default page - Select a default page from the drop down menu provided.
 - Allow Sponsor to change - Choose yes or no from the drop down menu.
- 12. Click on the Save button to save all changes.**

Sponsor Preferences

Configuring RADIUS Clients

This chapter describes the following:

- Overview
- Adding RADIUS Clients
- Editing RADIUS Clients
- Deleting RADIUS Clients
- Support Syslog for RADIUS accounting

Overview

Remote Authentication Dial In User Service (RADIUS) is an AAA (authentication, authorization and accounting) protocol. FortiConnect uses the RADIUS protocol to authenticate and audit Users who login through RADIUS-capable network enforcement devices, such as Wireless LAN Controllers.

When a User authenticates against a RADIUS client, such as a Wireless LAN Controller, the RADIUS client performs a RADIUS authentication check with FortiConnect to validate whether the credentials supplied by the user/device are valid. If the User authentication is successful, FortiConnect returns a message stating that the user is valid and the duration of time remaining before the user session expires. The RADIUS client must honour the session-timeout attribute to remove the User when the account time expires (unless the account is unlimited).

Note: The Wireless LAN Controller needs to be specifically configured to Allow AAA Override. This enables it to honour the session-timeout attribute returned to it by FortiConnect.

In addition to authentication, the RADIUS client device reports details to FortiConnect, such as the time the session started, time session ended, user IP address, and so on. This information is transported over the RADIUS Accounting protocol.

TIP - If there is a Firewall between FortiConnect and the RADIUS client, you need to allow traffic from UDP Port 1812 or 1645(RADIUS authentication) and UDP Port 1813 or 1646 (RADIUS accounting) to pass.

Note: The Debug button under Devices > RADIUS Clients turns the RADIUS server on in debugging mode. This enables detailed debug information to be viewed under Server > System Logs > Support Logs. See Support Logs for additional details.

Adding RADIUS Clients

1. From the administration interface, select Devices > RADIUS Clients from the left hand menu.
2. Before adding a RADIUS client you can determine whether you wish RADIUS authentication to be performed in a case sensitive or insensitive manner as show in the screen shot below. From the drop down menu in the RADIUS Authentication section, select the option you wish authenticate the RADIUS username in.
3. In the RADIUS Clients page as shown below, click the Add RADIUS Client button to add a RADIUS client.

RADIUS Clients

RADIUS Clients

Name	Device	Type	Description
No RADIUS Clients defined			

Add RADIUS Client

RADIUS Debug

RADIUS Support logs can be found in [Reports & Logs > System Logs > Support Logs](#)

RADIUS is running normally.

Restart RADIUS in Debug

RADIUS Authentication

This setting controls whether RADIUS authentication is performed in a case sensitive or insensitive manner.

RADIUS username is case sensitive

Save

4. In the Add RADIUS page, click on the Client tab as shown below, type a descriptive Name for the RADIUS client.

5. In Name - Type the name of the RADIUS Client
6. In Device IP Address / Prefix Length- Type the IP Address / Prefix Length of the RADIUS client, if you do not know the Prefix Length, the FortiConnect will automatically enter this for you. This needs to match the IP address from which the RADIUS request is originated.
7. Type a shared Secret for the RADIUS client. This must match the shared secret specified in the configuration of the RADIUS client.
8. Retype the shared secret in the Confirm field.
9. From the Type drop down menu select the type or vendor of the RADIUS client, if you select Fortinet, an extra tab will appear at the end of the set of tabs on the screen called Automatic Setup, for details on this screen goto step 22 for details on how to configure the options within.

Note: If selecting Generic Radius Device an Guest Portal along the top will appear, see step 18 for details on this.

Note: Depending on the Type of Radius Device you select, the options on this screen may differ slightly.

10. Type a Description of the client and any other information needed.
11. To turn on the use of Change-of-Authorization then place a check in the Use COA box.
12. Click the Save Button and the system will automatically restart and save the settings. Please wait whilst this occurs.
13. If you want the RADIUS client to send any additional attributes upon successful authentication, click on the Attributes tab as shown in the figure below.

Adding RADIUS Clients

The screenshot shows the 'RADIUS Clients' configuration window. The 'Attributes' tab is selected. The 'Vendor' dropdown is set to 'IETF'. The 'Attribute' dropdown is set to 'Access-Loop-Encapsulation'. The 'Value' field is empty. There is an 'Add AV Pair' button. Below the 'Value' field is a table with one empty row. To the right of the table are 'Move up', 'Remove', and 'Move down' buttons. At the bottom are 'Save' and 'Cancel' buttons.

14. You can use the drop down menus to select :

- Vendor - A list of predefined Vendors are available using the drop down menu.
- Attribute - A list of predefined Attributes will appear depending on what Vendor you selected, use the drop down menu to select the appropriate one.
- Value - Enter the appropriate value in the field provided.

15. Click on the Add AV Pair button to add attribute and value pair to the table below.

- If you want to remove an attribute, select the attribute from the table and click the Remove button.
- Use the Move up and Move down buttons to change the order of the RADIUS attributes as they are sent in the RADIUS Accept Message.

16. Click the Save Button and the system will automatically restart and save the settings. Please wait whilst this occurs.

Note: FortiConnect supports TLS, PAP, CHAP, PEAP-MSCHAPv2 and PEAP-GTC in RADIUS Authentication

Note: SNMP is used for recording the Framed-IP-Address of the guest when the RADIUS client does not set this in RADIUS accounting messages. You do not need to set this if the device sets it correctly.

17. To set this click on the SNMP tab as shown in the figure below

RADIUS Clients

Client | Attributes | **SNMP** | MAC Authentication | RadSec Authentication | Automatic Setup

SNMP is used for recording the Framed-IP-Address of the guest when the RADIUS client does not set this in RADIUS accounting messages. You do not need to enable this if the device sets it correctly.

Enable: ☒

Alternative SNMP device IP Address: If the RADIUS Client doesn't support SNMP access to the ARP table, query this device instead

Version: **V3** V2c & V3 perform better than V1

Read Community:

Authentication Protocol: **MD5**

Authentication Username:

Authentication Passphrase: Confirm:

Privacy Protocol: **DES**

Privacy Passphrase: Confirm:

Security Type: **Authentication**

Save **Cancel**

18. Place a check in the enable check box.

- Version - Select the correct version number from the drop down box.
- Read Community - Enter the read community string.
- Authentication Protocol - Select the correct authentication protocol from the drop down box.
- Authentication Username - Enter the authentication username.
- Authentication Passphrase - Enter the authentication passphrase and confirm it in the field provided.
- Privacy Protocol - Select the correct privacy protocol from the drop down menu provided.
- Privacy Passphrase - Enter the privacy passphrase and confirm it in the field provided.
- Security Type - Select the correct security type from the drop down menu provided.

Click the Save button and the system will automatically restart and save the settings. Please wait whilst this occurs.

To set up and enable MAC Authentication, click on the MAC Authentication tab as shown below.

The screenshot shows the 'RADIUS Clients' configuration interface. At the top, there's a blue header bar with the text 'RADIUS Clients'. Below it, a tabbed interface is visible with tabs for 'Client', 'Attributes', 'SNMP', 'MAC Authentication' (which is the active tab), 'RadSec Authentication', and 'Automatic Setup'. The 'MAC Authentication' tab contains the following settings:

- 'Enable MAC authentication:' with a checked checkbox.
- 'User-Name attribute contains:' with a dropdown menu set to 'Client MAC Address'.
- 'User-Password attribute contains:' with a dropdown menu set to 'Shared Secret'.
- 'Service-Type attribute contains:' with a dropdown menu set to 'Login-User'.

At the bottom of the configuration area, there are two buttons: 'Save' and 'Cancel'.

Note: MAC Auth settings depend on what the controller sends when it does a MAC Auth request

19. Place a check in the Enable MAC authentication check box :-

- User-Name attribute contains - From the drop down menu select whether the User Name attribute contains Client MAC Address, Shared Secret, whether its Not Present, or Don't Check.
- User-Password attribute contains - From the drop down menu select whether the User Password attribute contains Client MAC Address, Shared Secret, whether its Not Present, or Don't Check.
- Service-Type attribute contains - From the drop down menu select whether the Service Type attribute should contain the Login User, Call Check, or Don't Check.

20. Click on Save once complete.

21. When creating certain client of 'Type' the tab below is shown

The setting on the tab can allow a generic RADIUS client to interface with a Portal by providing login/logout parameters and request keys

Enter the relevant settings to allow the RADIUS client to interface with a Portal :

- Method - Choose the HTTP method with which forms are submitted to the Generic RADIUS device.
- Login URL - Enter the URL used to login users to the device
- Username request key - Enter the username key, this normally corresponds to the name of the HTML element that takes the username.
- Password request key - Enter the password key
- Redirection request key - Enter the redirect key
- Custom Login Parameters - Enter any custom login parameters the device may require.
- Logout URL - Enter the URL used to logout users on the device.
- Custom Logout Parameters - Enter any custom logout parameters the device may require.

Click on the Save button once completed.

22. If you are adding RADIUS for authentication with a Fortinet Controller you will see the tab as shown below.

Adding RADIUS Clients

RADIUS Clients

⚠ The Meru Connect is using a self-signed SSL certificate, you may get certificate warnings on your clients when they attempt to authenticate

Client Attributes SNMP MAC Authentication RadSec Authentication **Automatic Setup**

Meru Connect Address: 192.168.137.20
This hostname is used to redirect guests to the Meru Connect, it should match the SSL certificate on Meru Connect.

Device IP Address: 10.10.1.2

Admin user name:

Admin Password:

Configure RADIUS profiles: ☒

Set Captive Portal RADIUS profiles: ☒

Set Captive Portal External URL: ☒

Configure QoS Rules: ☒

Write changes to startup-config: ☐ This will overwrite your startup-config with the current running-config

Setup Controller

23. Within this tab you can automate several configuration steps between FortiConnect and the Fortinet Controller. Steps you previously took when setting up the client and SNMP will also be automated once you click on the Setup Controller button :-

- FortiConnect Address - Enter the IP Address of FortiConnect (should match the SSL cert common name)
- Device IP Address - Enter the IP Address of the controller, this can be IP address or FQDN
- Admin User Name - Enter the admin user name for the controller
- Admin Password - Enter the admin password for the controller
- Configure RADIUS Profiles - Check the box to Configure RADIUS profiles for authentication and account
- Set Captive portal RADIUS profiles - Check the box to set captive portal RADIUS profiles
- Set Captive portal mode - Check the box to set the captive portal mode to customized
- Configure QoS Rules - Check the box to configure Pre Authentication QoS Rules
- Transfer Pages to Controller - Check the box to transfer portal redirection pages to controller
- Write changes to startup-config- Check the box to write changes to startup config.

24. Click on the Setup Controller button to apply the selection confirmation to the controller.

25. Click on the Download portal pages link for manual upload to the RADIUS client

Note: System Director 6.0 & Later - for versions of System Director 6.0 and later we configure the Captive Portal External URL with a redirection URL pointing to FortiConnect. Also, Automatic Setup no longer requires you to Transfer Custom Portal Pages from FortiConnect to the controller, Set the Captive Portal Mode to Customized and Set the Captive Portal Authentication Method to Internal as shown in the screenshot below.

Identity Manager Address:
This hostname is used to redirect guests to the Identity Manager, it should match the SSL certificate on Identity Manager.

Device IP Address:

Admin user name:

Admin Password:

Configure RADIUS profiles: ☒

Set Captive Portal RADIUS profiles: ☒

Set Captive Portal External URL: ☒

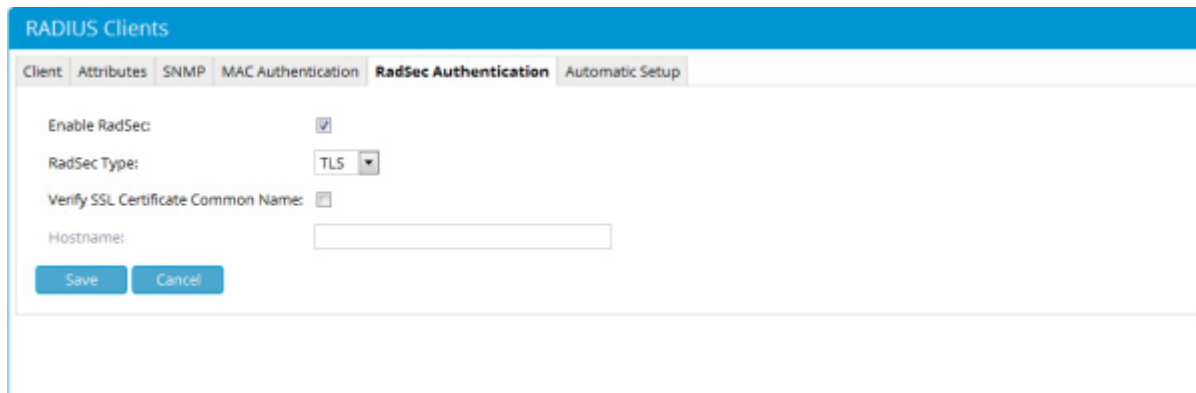
Configure QoS Rules: ☒

Write changes to startup-config: ☐ This will overwrite your startup-config with the current running-config

RadSec Authentication

The main focus of RadSec is to provide a means to secure the communication between RADIUS/TCP peers on the transport layer. The most important use of RadSec lies in roaming environments where RADIUS packets need to be transferred through different administrative domains and untrusted, potentially hostile networks. An example for a world-wide roaming environment that uses RadSec to secure communication is Eduroam of which FortiConnect supports (see Network Access Policy section for Eduroam)

To enable RadSec Authentication on your RADIUS client go to Devices --> RADIUS Clients and click on the RadSec Authentication tab as shown below.



The screenshot shows the 'RADIUS Clients' configuration window with the 'RadSec Authentication' tab selected. The window has a blue header bar with the title 'RADIUS Clients'. Below the header is a tabbed interface with five tabs: 'Client', 'Attributes', 'SNMP', 'MAC Authentication', 'RadSec Authentication' (which is active), and 'Automatic Setup'. The 'RadSec Authentication' tab contains the following settings:

- 'Enable RadSec': A checkbox that is checked.
- 'RadSec Type': A dropdown menu with 'TLS' selected.
- 'Verify SSL Certificate Common Name': A checkbox that is unchecked.
- 'Hostname': An empty text input field.
- 'Save' and 'Cancel' buttons at the bottom left.

1. Click the Enable RadSec checkbox to enable RadSec
2. From the RadSec Type dropdown menu, select TLS or DTLS as your RadSec type.
3. Click the Verify SSL Certificate Common Name checkbox to enable verification.
4. Enter the RADIUS Client Hostname in the field provided.
5. Click Save to continue.

Editing RADIUS Clients

1. From the administration interface, select Devices > RADIUS Clients from the left hand menu.
2. In the RADIUS Clients page as shown below, select the RADIUS client from the list you wish to edit and click the underlined name of that client.

RADIUS Clients

RADIUS Clients

Name	Device	Type	Description	
RADIUS 1	10.10.1.2/32	Meru SD 6.0 & Later	RADIUS 1	

[Add RADIUS Client](#)

RADIUS Debug

RADIUS Support logs can be found in [Reports & Logs > System Logs > Support Logs](#)

RADIUS is running normally.

[Restart RADIUS in Debug](#)

RADIUS Authentication

This setting controls whether RADIUS authentication is performed in a case sensitive or insensitive manner.

RADIUS username is case sensitive ▼

[Save](#)

3. In the Edit RADIUS Client page as shown below, click on the tabs you wish to Edit and follow the instructions as shown in Adding RADIUS Clients.


Click on Save once complete.

Deleting RADIUS Clients

1. From the administration interface, select Devices > RADIUS Clients from the left hand menu.

RADIUS Clients

RADIUS Clients

Name	Device	Type	Description	
<u>RADIUS 1</u>	10.10.1.2/32	Meru SD 6.0 & Later	RADIUS 1	

Add RADIUS Client

RADIUS Debug

RADIUS Support logs can be found in [Reports & Logs > System Logs > Support Logs](#)

RADIUS is running normally.

Restart RADIUS in Debug

RADIUS Authentication

This setting controls whether RADIUS authentication is performed in a case sensitive or insensitive manner.

RADIUS username is

Save

-
2. In the RADIUS Clients page as shown above, click the underlined name of the RADIUS client in the list to edit it.
3. Click the dustbin icon to the right of the entry to delete it, and confirm the action.

RADIUS Accounting Servers

To add a RADIUS Accounting Server go to Devices --> RADIUS Accounting Servers and click on the Add RADIUS Accounting Server button as shown below. FortiConnect can replicate and forward any accounting packets to an admin defined server.

RADIUS Accounting Servers

Name	Device	Action
No RADIUS Accounting servers defined		

[Add RADIUS Accounting Server](#)

User-Name Format

Modify User-Name values: ☐

Realm:

Leave empty to use the realm the user authenticated with

Authenticate with:

- ☐ realm/username
- ☐ realm/username
- ☐ username@realm
- ☒ username

[Save](#)

1. On the Add RADIUS Accounting Server, enter the server details you wish to forward accounting packets to.

RADIUS Accounting Server

Name:

Server IP Address:

Secret: Confirm:

Accounting Port:

[Save](#) [Cancel](#)

2. In the fields provided, enter :-
 - Name - The name of the RADIUS Accounting Server
 - Server IP Address - The IP Address of the RADIUS Accounting Server

- Secret - The shared Secret of the RADIUS Accounting Server
 - Confirm - Confirm the shared Secret
 - Accounting Port - The Accounting Port
3. Click on Save once complete
 4. If you wish to Modify the User-Name value of your server, then place a check in the Modify User-Name value check box as shown below.

RADIUS Accounting Servers

Name	Device	Action
RADACC	10.10.1.2	

[Add RADIUS Accounting Server](#)

User-Name Format

Modify User-Name value: ☒

Realm:

Leave empty to use the realm the user authenticated with

Authenticate with:

- ☐ realm/username
- ☐ realm/username
- ☐ username@realm
- ☒ username

[Save](#)

5. Realm - Enter the Realm details
6. Authenticate with - Place a check next to the format you wish to authenticate with
7. Click on Save to complete your changes

Edit a RADIUS Accounting Server

1. To Edit a RADIUS Accounting Server go to Devices --> RADIUS Accounting Servers and click on the link of the RADIUS Accounting Server you wish to edit as shown below

RADIUS Accounting Servers

RADIUS Accounting Servers

Name	Device	Action
RAD.ACC	10.10.1.2	

[Add RADIUS Accounting Server](#)

User-Name Format

Modify User-Name values: ☒

Realm:
Leave empty to use the realm the user authenticated with

Authenticate with:

- ☐ realm\username
- ☐ realm/username
- ☐ username@realm
- ☒ username

[Save](#)

2. Follow steps 2 and 3 in the Add RADIUS Accounting Server section to Edit the server.

Delete a RADIUS Accounting Server

1. To Delete a RADIUS Accounting Server go to Devices --> RADIUS Accounting Servers and click on the Bin Icon of the RADIUS Accounting Server you wish to delete as shown below

Name	Device	Action
RAD ACC	10.10.1.2	

Add RADIUS Accounting Server

User-Name Format

Modify User-Name value: ☒

Realm:
Leave empty to use the realm the user authenticated with

Authenticate with:

- ☐ realm/username
- ☐ realm/username
- ☐ username@realm
- ☒ username

Save

2. Click on OK to delete the server details or click on Cancel to abort.

Syslog for RADIUS Accounting

FortiConnect can send RADIUS accounting information as Syslog messages to a firewall's and other devices to allow access to the client once they have logged onto the network via FortiConnect.

1. From the FortiConnect Administration interface go to Devices --> Syslog Servers.

M

Syslog Servers

When RADIUS accounting is received a syslog message is sent to these servers.

Message Format: Smoothwall Firewall ▼

IP Address	Port
There is no syslog server configured to send messages to	
<input type="text"/>	514 <input type="button" value="Add"/>

2. Select how the Syslog message should be formatted by selecting the Message Format from the drop down menu -
3. Smoothwall Firewall - this option will apply predefined format as under:
 - Start = "name=%{User-Name} mac=%{Calling-Station-Id} ip=%{Framed-IP-Address} \$"
 - Stop = "name=%{User-Name} mac=%{Calling-Station-Id} ip=%{Framed-IP-Address} \$"
 - Interim = "name=%{User-Name} mac=%{Calling-Station-Id} ip=%{Framed-IP-Address} \$"
4. Custom - this option lets admin define format against each point e.g Start, Stop and Interim as shown below.

Syslog Servers

When RADIUS accounting is received a syslog message is sent to these servers.

Message Format: Custom

Start:

Stop:

Interim:

IP Address	Port
There is no syslog server configured to send messages to	
<input type="text"/>	<input type="text" value="514"/>
<input type="button" value="Add"/>	

- Once completed click on Save to continue, this will send a message to all configured servers in this format.
- Now add a syslog server to send messages to -
- Enter the server IP Address and the Port number, click on the Add button once complete.
- Click on Save.

FortiConnect LDAP Server

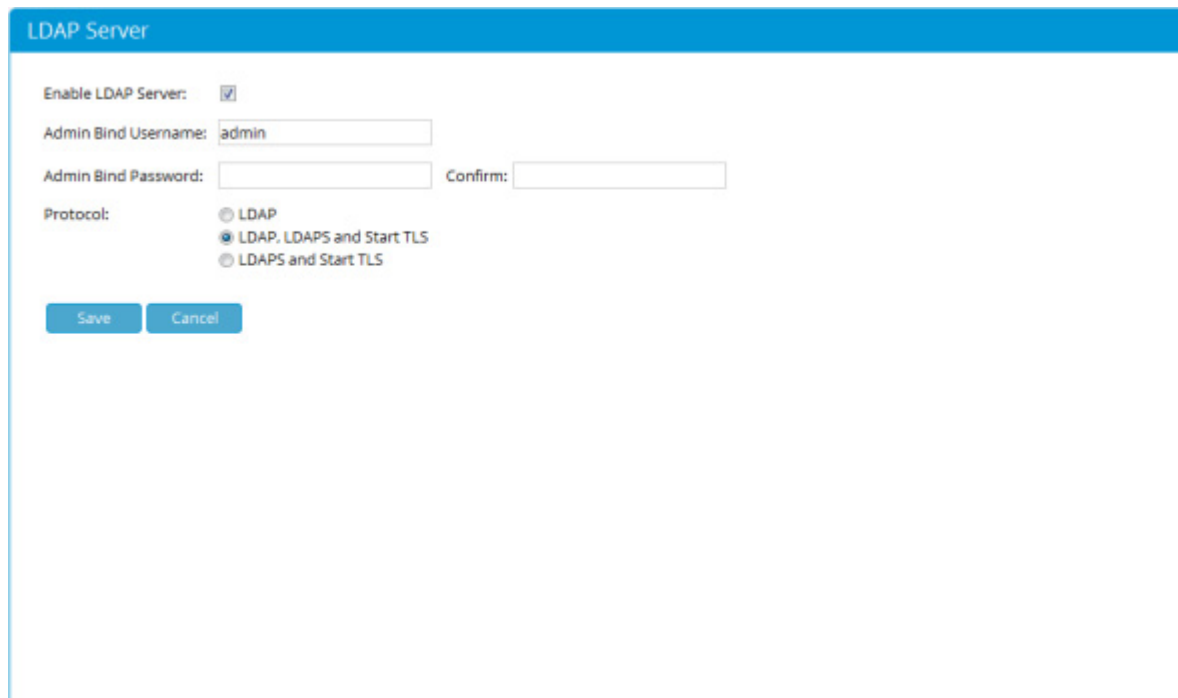
FortiConnect has a built-in LDAP server that exposes User and Device accounts to applications that use the LDAP for User authentication and Device validation.

Note: It is also possible to use the LDAP server to browse the current active User and Device accounts. This is unrelated to using an external LDAP server for Sponsor authentication.

Configuring the FortiConnect LDAP Server

Administer the FortiConnect LDAP Server by following the steps below.

1. From the administration interface select Devices --> LDAP Server and place a tick inside the Enable LDAP Server check box as shown below.



The screenshot shows the 'LDAP Server' configuration page in FortiConnect. The page has a blue header bar with the text 'LDAP Server'. Below the header, there are several configuration fields and a 'Protocol' section. The 'Enable LDAP Server' checkbox is checked. The 'Admin Bind Username' field contains the text 'admin'. The 'Admin Bind Password' and 'Confirm' fields are empty. The 'Protocol' section has three radio button options: 'LDAP', 'LDAP, LDAPS and Start TLS' (which is selected), and 'LDAPS and Start TLS'. At the bottom of the form, there are two buttons: 'Save' and 'Cancel'.

LDAP Server

Enable LDAP Server: ☒

Admin Bind Username:

Admin Bind Password: Confirm:

Protocol:

- ☐ LDAP
- ☒ LDAP, LDAPS and Start TLS
- ☐ LDAPS and Start TLS

2. Create an Admin Bind Username in the field provided.
3. Create an Admin Bind Password and Confirm in the fields provided.
4. Select the required protocol by placing a check in the relevant check box.
 - LDAP - Allow Unencrypted only.
 - LDAP, LDAPS and Start TLS - Allow Unencrypted and encrypted.
 - LDAPS and Start TLS - Allow encrypted only.
5. Click on Save once you have finished.

Using the FortiConnect LDAP Server

Authenticating a User Account via LDAP

To authenticate a user account the client must bind to the LDAP server using the bind DN and password of the User account. The bind DN is always of the form:

```
cn=username,ou=users,dc=MeruConnect
```

where username is that of the user account. For example if we have a user account with username “test” the bind DN would be:

```
cn=test,ou=users,dc=MeruConnect
```

The base DN for searching is always:

```
ou=users,dc=MeruConnect
```

Users can only be authenticated if they are active and are not currently under any time restrictions.

Troubleshooting User Authentication

We can use command-line tools and graphical tools to test the behaviour of the LDAP server. For example if the `ldapsearch` command is available on a client machine we can test authentication using the following (where `testpassword` and `testusername` are the users credentials and `x.x.x.x` is the IP address of the FortiConnect server):

```
ldapsearch -h x.x.x.x -x -D "cn=testusername,ou=users,dc=MeruConnect" -w testpassword
```

This will return all the detail of the account, including the DN:

```
dn: cn=test,ou=users,dc=MeruConnect
```

If the username or password is incorrect it will return:

```
ldap_bind: Invalid credentials (49)
```

Validating a Device Account via LDAP

Device accounts may be validated in a similar way to User accounts, however device accounts do not have passwords so we must use the admin bind credentials to search for the existence of a device account.

The device DN is always of the form:

```
cn=aa:bb:cc:dd:ee:ff,ou=Devices,dc=MeruConnect
```

Where the CN is the MAC address of the device in a canonical format.

We may search for a device using `ou=Devices,dc=MeruConnect` as the base DN and `cn=aa:bb:cc:dd:ee:ff` as the filter.

Many other MAC address formats are supported for searching, the `altMacAddressFormat` attribute should be used e.g. using a filter of `altMacAddressFormat=aabb-ccdd-eeff`.

Testing Device Validation

We can use command-line tools and graphical tools to test the behaviour of the LDAP server. For example if the `ldapsearch` command is available on a client machine we can test validation of device accounts with the following (where `x.x.x.x` is the IP address of the FortiConnect server and `adminuser` and `adminpassword` are the admin bind username and password respectively and we assume we have a device with a MAC address of `aa:bb:cc:dd:ee:ff`):

```
ldapsearch -h x.x.x.x -LLL -x -D "cn=adminuser,dc=MeruConnect" -w adminpassword  
(cn=aa:bb:cc:dd:ee:ff)
```

This will return all the details of the device, including:

```
dn: cn=aa:bb:cc:dd:ee:ff,ou=Devices,dc=MeruConnect
```

If the username or password is incorrect it will return:

```
ldap_bind: Invalid credentials (49)
```

It will not display any results if the device is not found.

Browsing Guest and Device Accounts

While configuring clients that access the LDAP server it may be useful to view the LDAP

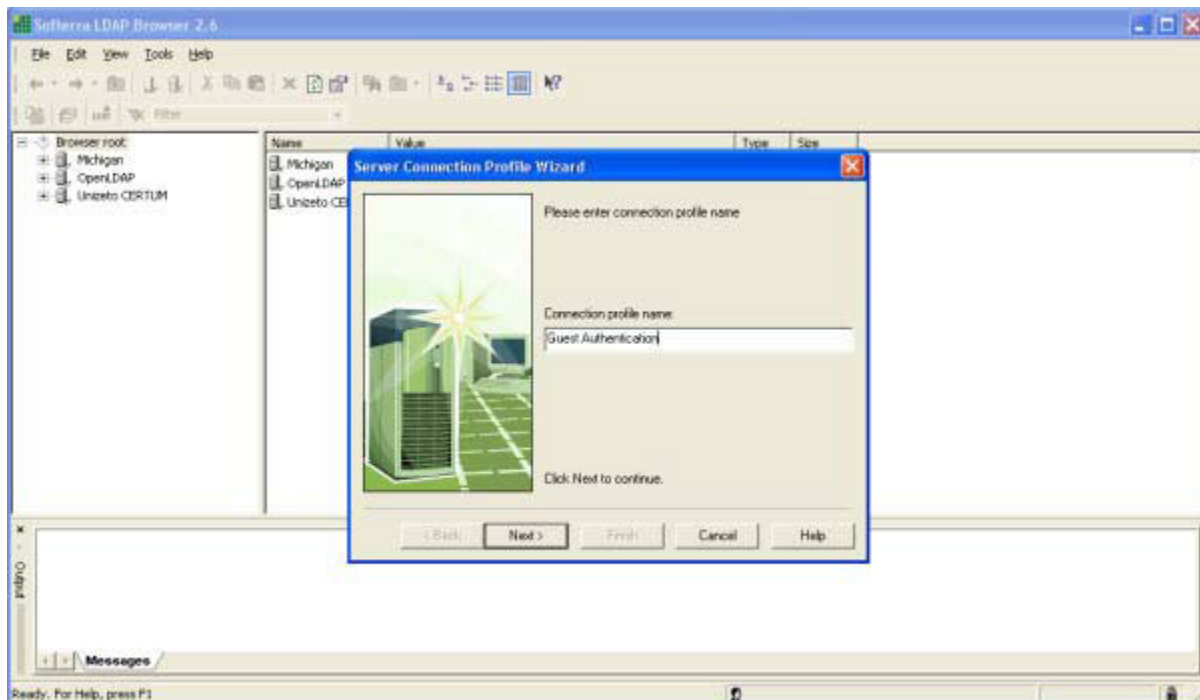
database using a LDAP browsing application. The following screenshots are taken of the free LDAP Browser application from Softera (<http://www.ldapadministrator.com>).

In the examples that follow the FortiConnect is running on 192.168.137.20 and the LDAP server has been configured with the username “admin” and password “password”:


- Guest Authentication
- Device Validation
- Browsing

User Authentication

1. Click on File then New Profile from the drop down menus and select Create New File and name it Guest Authentication



2. Click Next
3. Host - IP Address of the FortiConnect
4. Leave the Port and Protocol version as they appear.
5. Base DN = ou=Guests,dc=GuestManager



The image shows a 'Host Information' dialog box with a blue title bar and a close button. On the left is a graphic of a server rack. The main area has a light beige background with the text 'Please enter server host information'. It contains several input fields: 'Host' with the value '192.168.137.20', 'Port' with '389', and 'Protocol version' with a dropdown set to '3'. The 'Base DN' dropdown is set to 'ou=Guests,dc=GuestManager'. Below these is a 'Fetch DN's (only LDAP v.3)' button. An 'Anonymous bind' checkbox is unchecked. A message 'Click Next to continue.' is at the bottom left. At the bottom are five buttons: '< Back', 'Next >', 'Finish', 'Cancel', and 'Help'.

Host Information

Please enter server host information

Host: 192.168.137.20

Port: 389 Protocol version: 3

Base DN: ou=Guests,dc=GuestManager

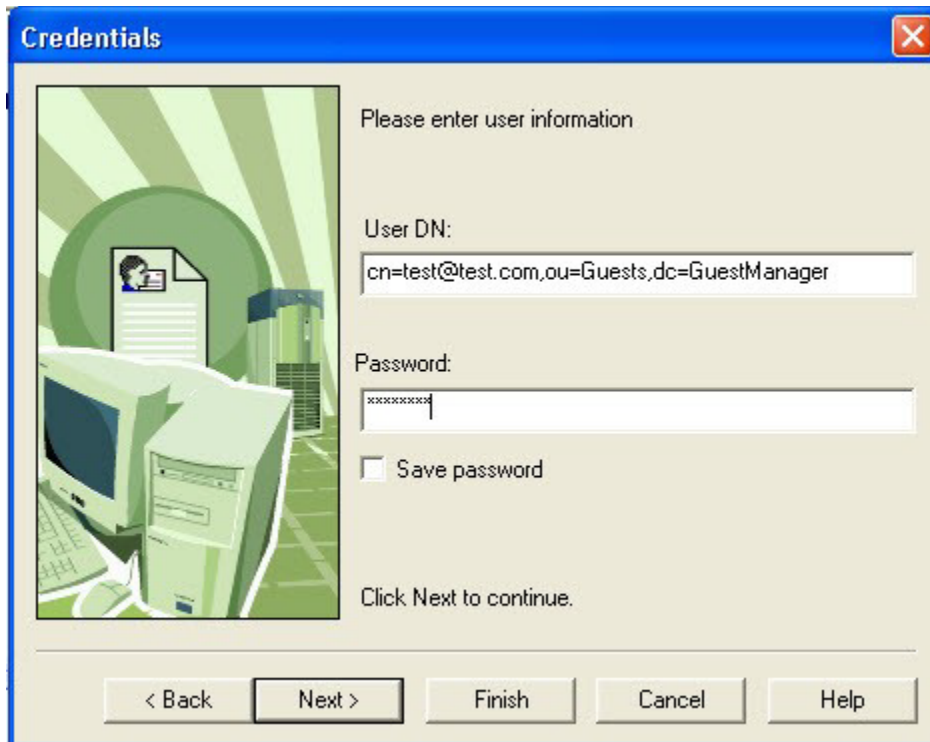
Fetch DN's (only LDAP v.3)

☐ Anonymous bind

Click Next to continue.

< Back Next > Finish Cancel Help

6. Click Next
7. User DN = Guest User DN
8. Password = Guest User Password
9. Click on the check box to Save Password.



The 'Credentials' dialog box has a blue title bar with a close button. On the left is a green-tinted illustration of a computer monitor, tower, and a document with a person's icon. The main area is light beige and contains the text 'Please enter user information'. Below this are two input fields: 'User DN:' with the value 'cn=test@test.com,ou=Guests,dc=GuestManager' and 'Password:' with a masked password 'xxxxxxxx'. A checkbox labeled 'Save password' is unchecked. At the bottom, it says 'Click Next to continue.' and has five buttons: '< Back', 'Next >', 'Finish', 'Cancel', and 'Help'.

Credentials

Please enter user information

User DN:
cn=test@test.com,ou=Guests,dc=GuestManager

Password:
xxxxxxxx

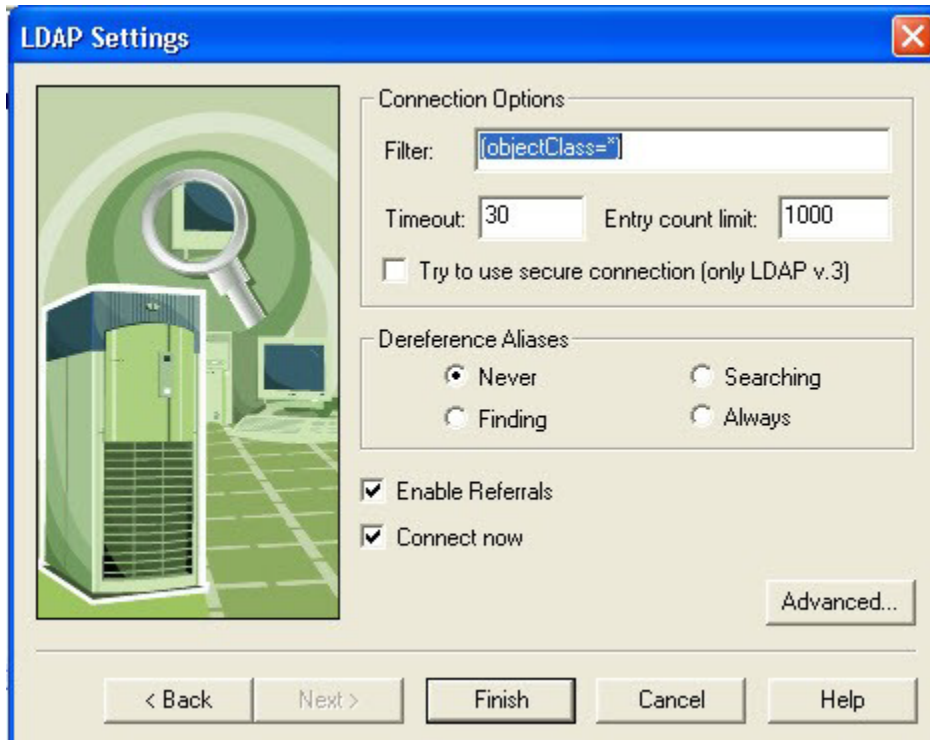
☐ Save password

Click Next to continue.

< Back Next > Finish Cancel Help

10. Click Next

11. Click Finish as shown below.



The 'LDAP Settings' dialog box has a blue title bar with a close button. On the left is a green-tinted illustration of a server rack with a magnifying glass over it. The main area is light beige and contains two sections: 'Connection Options' and 'Dereference Aliases'. 'Connection Options' includes a 'Filter:' field with '(objectClass=*)', 'Timeout:' set to '30', 'Entry count limit:' set to '1000', and an unchecked checkbox 'Try to use secure connection (only LDAP v.3)'. 'Dereference Aliases' has four radio buttons: 'Never' (selected), 'Finding', 'Searching', and 'Always'. Below these are two checked checkboxes: 'Enable Referrals' and 'Connect now'. An 'Advanced...' button is at the bottom right. At the very bottom are five buttons: '< Back', 'Next >', 'Finish', 'Cancel', and 'Help'.

LDAP Settings

Connection Options

Filter: (objectClass=*)

Timeout: 30 Entry count limit: 1000

☐ Try to use secure connection (only LDAP v.3)

Dereference Aliases

☒ Never ☐ Searching
☐ Finding ☐ Always

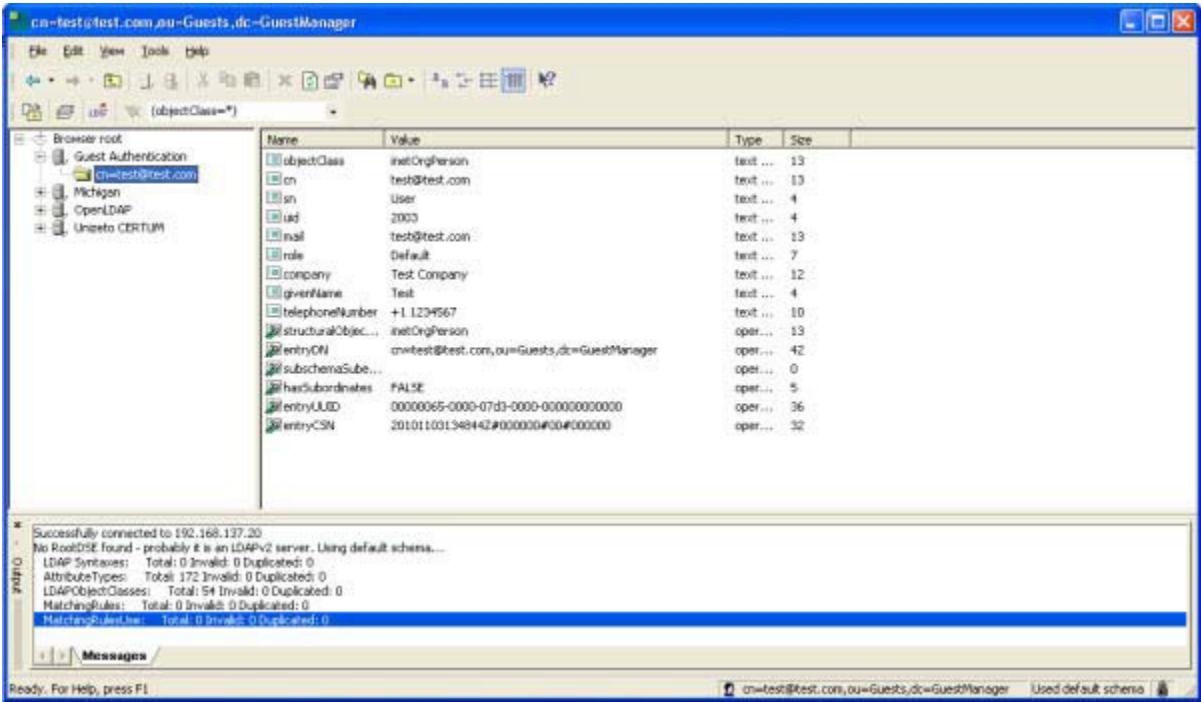
☒ Enable Referrals
☒ Connect now

Advanced...

< Back Next > Finish Cancel Help

Device Validation

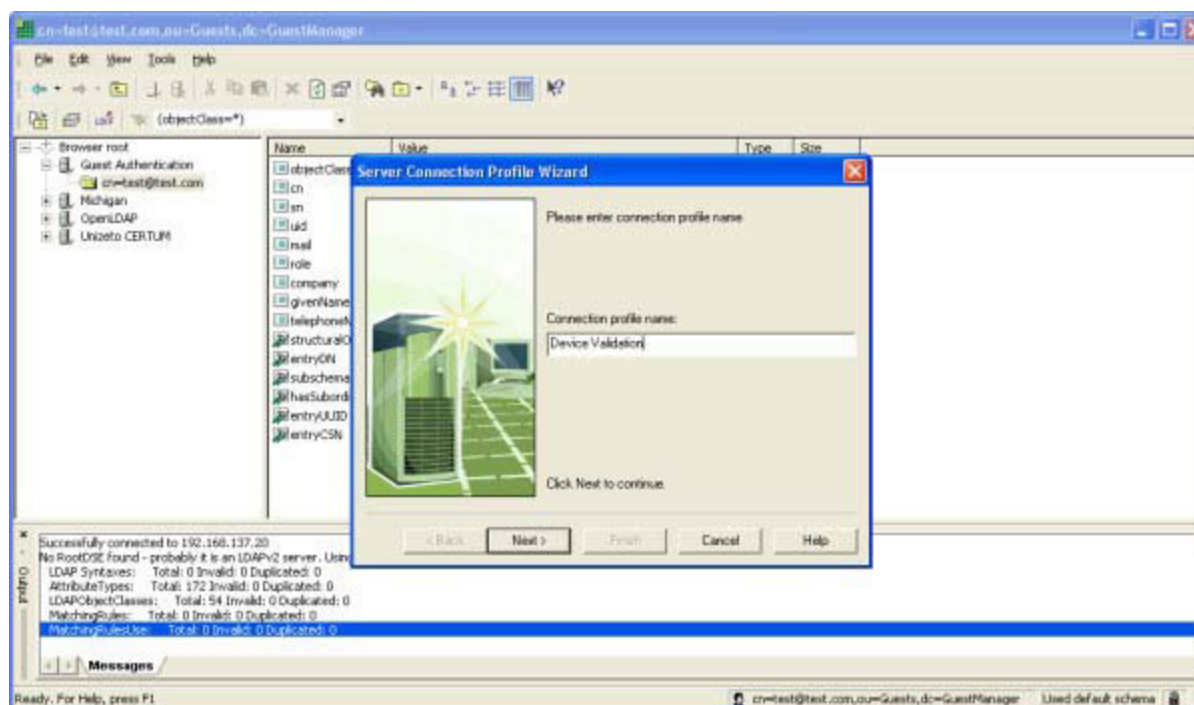
The results should be shown in the Guest Authentication folder.
Click on the folder to see the results and prove the Guest has authenticated.



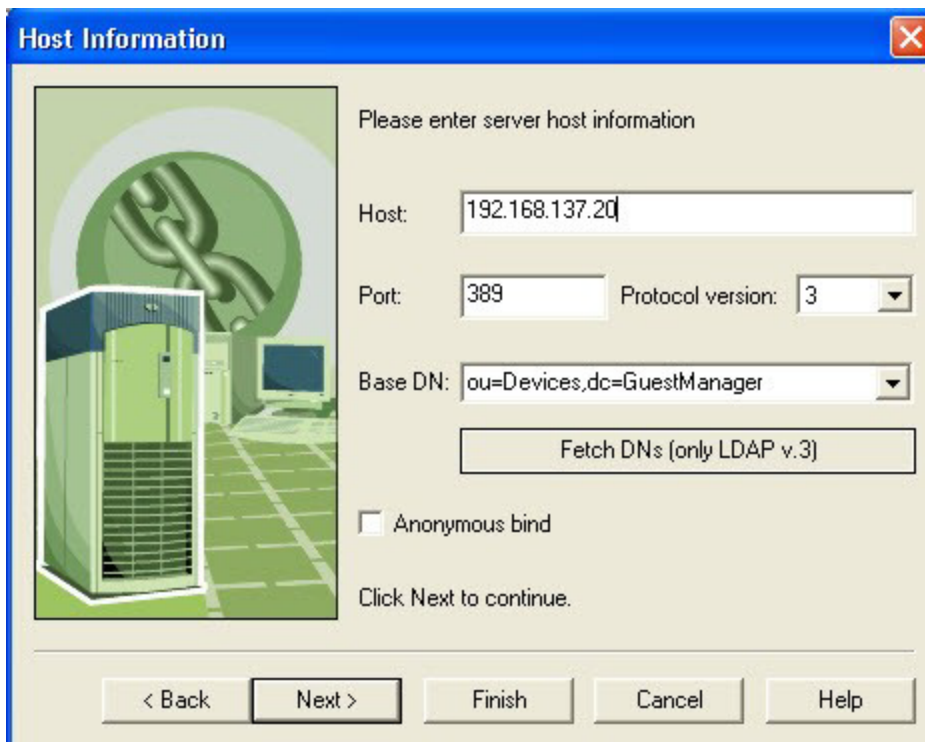
Device Validation

Device Validation

1. From the drop down menu select File-->New Profile and create a new profile called DeviceValidation.

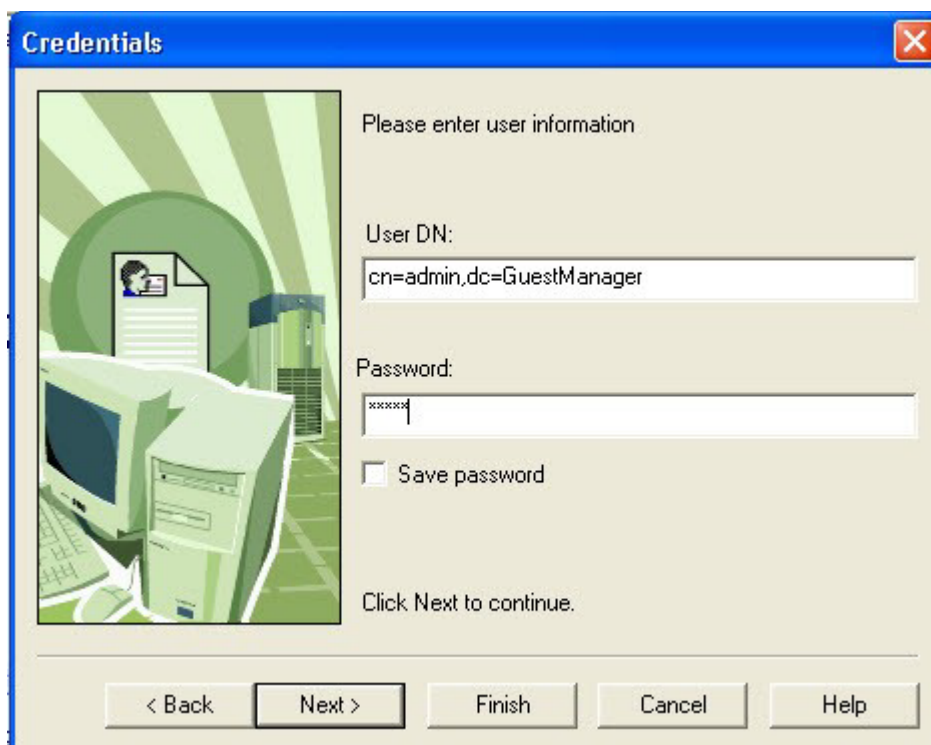


2. Click Next
3. Host - FortiConnect IP Address
4. Base DN - ou=Devices,dc=GuestManager
5. Port and Protocol remain how they are.



The image shows a Windows-style dialog box titled "Host Information". On the left is a graphic of a server rack. The main area contains the text "Please enter server host information". Below this are input fields for "Host:" (containing "192.168.137.20"), "Port:" (containing "389"), and "Protocol version:" (a dropdown menu set to "3"). Below these is a "Base DN:" dropdown menu containing "ou=Devices,dc=GuestManager". A button labeled "Fetch DN's (only LDAP v.3)" is positioned below the Base DN field. There is an unchecked checkbox labeled "Anonymous bind" and the instruction "Click Next to continue." at the bottom of the main area. At the very bottom of the dialog are five buttons: "< Back", "Next >", "Finish", "Cancel", and "Help".

6. Click Next
7. User DN, this is the username created when setting up LDAP FortiConnect - cn=Admin,dc=GuestManager
8. Password, this is the password created when setting up LDAP FortiConnect.



Credentials

Please enter user information

User DN:
cn=admin,dc=GuestManager

Password:
xxxxx

☐ Save password

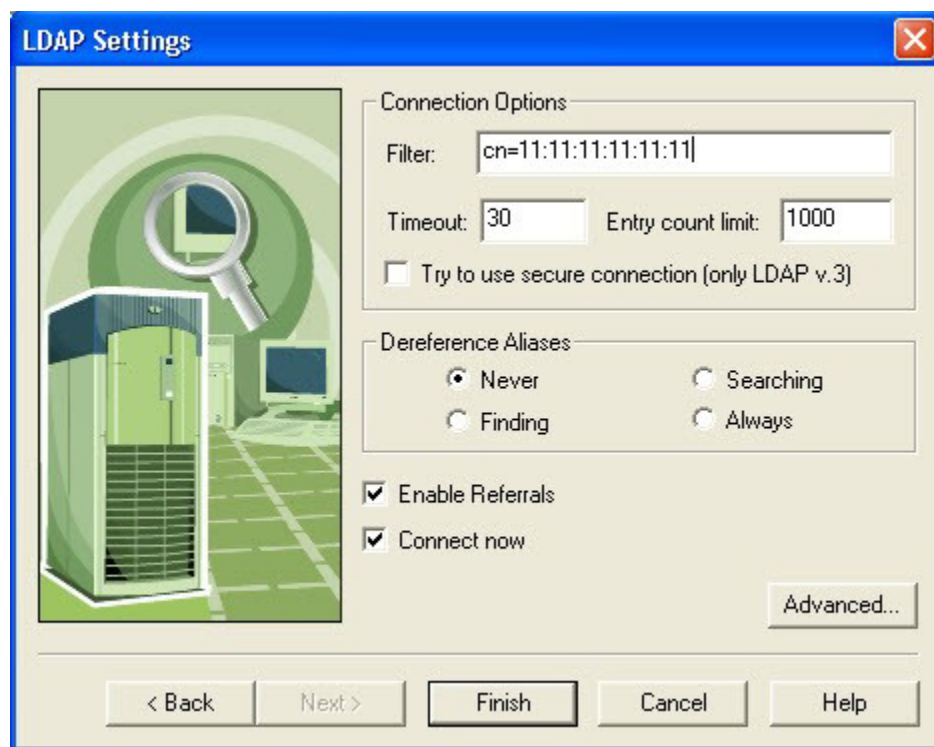
Click Next to continue.

< Back Next > Finish Cancel Help

9. Click Next

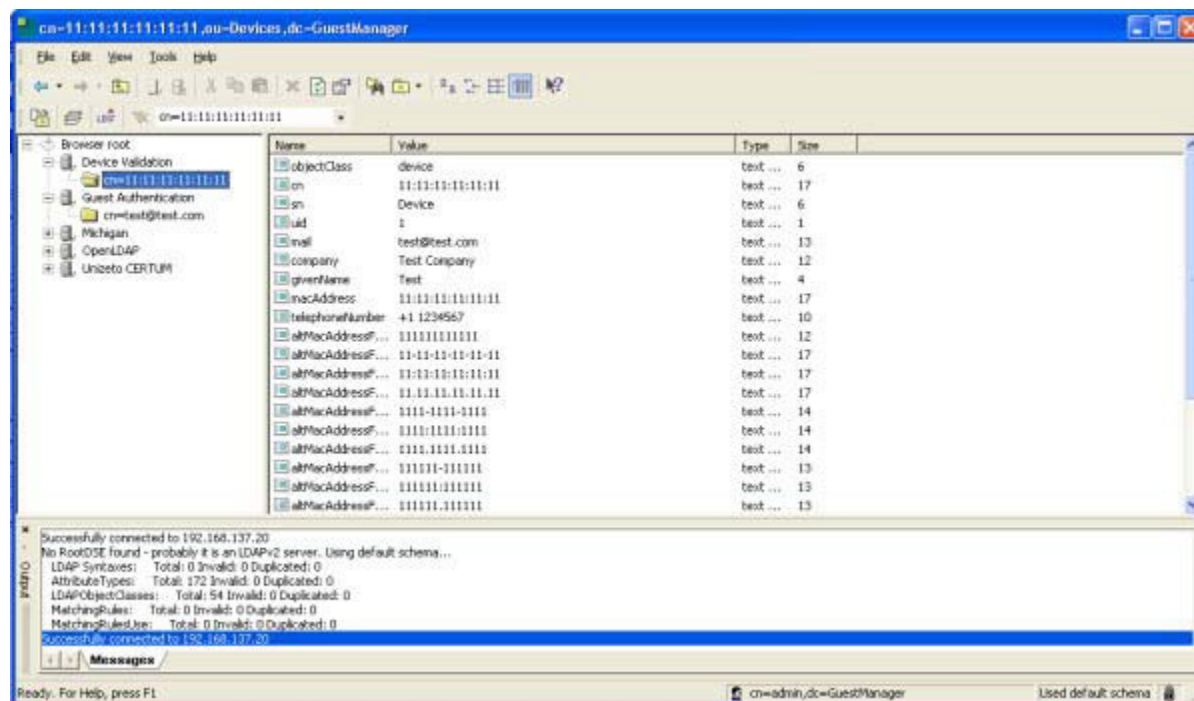
10. You must then setup a filter to find whether the Device exists. Filter - MAC Address of the Device.

11. Leave all other options as they are.



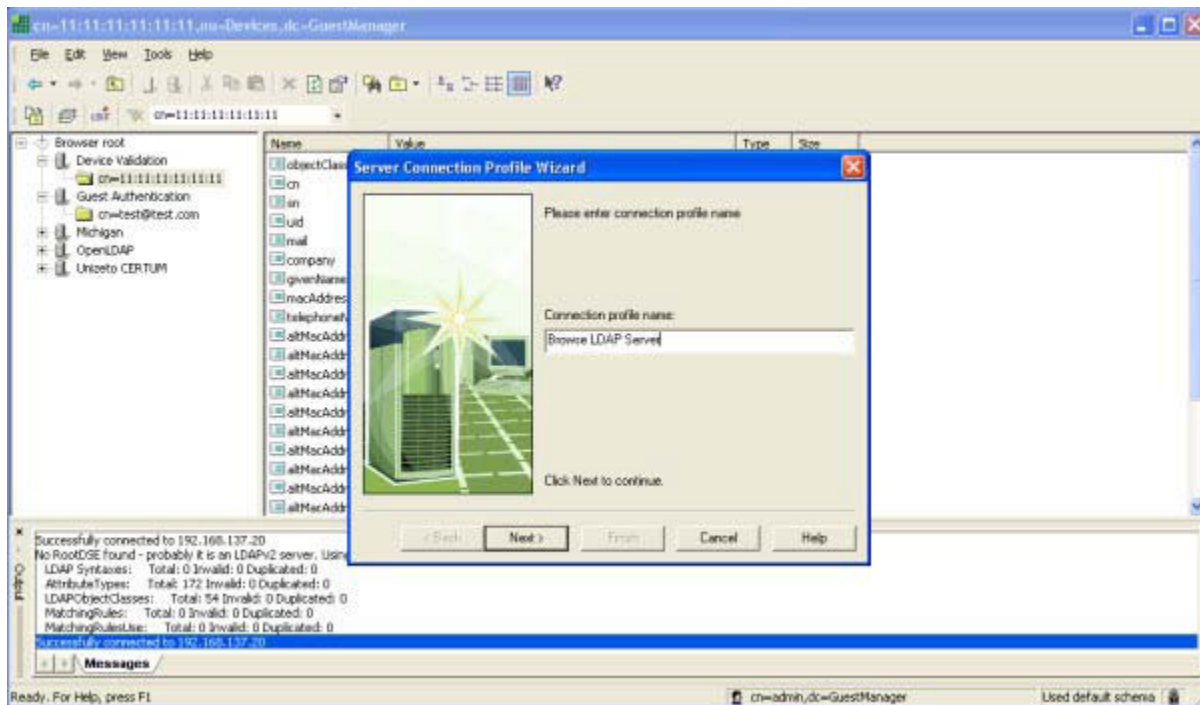
12. Click Finish

Under the Device Validation option on the menu, click on the Device Validation to prove the Device has validated as shown below.

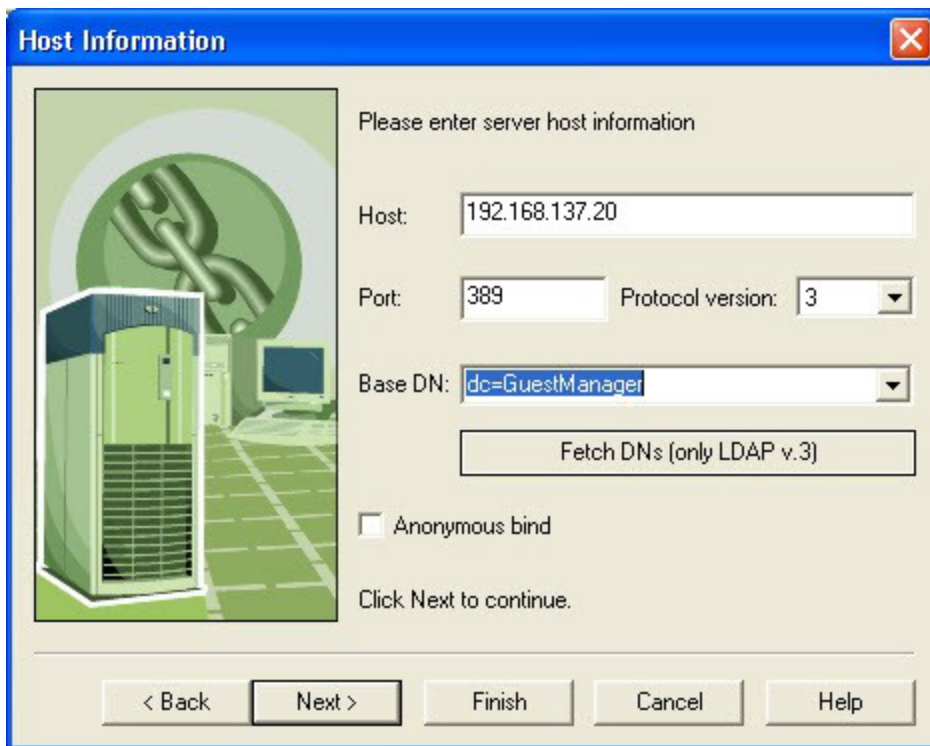


Browsing the LDAP Database

1. From the drop down menu select File-->New Profile and create a new profile called Browse LDAP Server.



2. Click Next
3. Host is the IP Address of your FortiConnect
4. Base DN is - dc=GuestManager
5. Leave the Port and Protocol settings as they appear.



The image shows a 'Host Information' dialog box with a blue title bar and a close button. On the left is a graphic of a server rack. The main area contains the text 'Please enter server host information'. There are input fields for 'Host' (192.168.137.20), 'Port' (389), and 'Protocol version' (3). A dropdown menu for 'Base DN' shows 'dc=GuestManager'. Below these is a 'Fetch DN's (only LDAP v.3)' button and an unchecked 'Anonymous bind' checkbox. At the bottom are buttons for '< Back', 'Next >', 'Finish', 'Cancel', and 'Help'. The text 'Click Next to continue.' is also present.

Host Information

Please enter server host information

Host: 192.168.137.20

Port: 389 Protocol version: 3

Base DN: dc=GuestManager

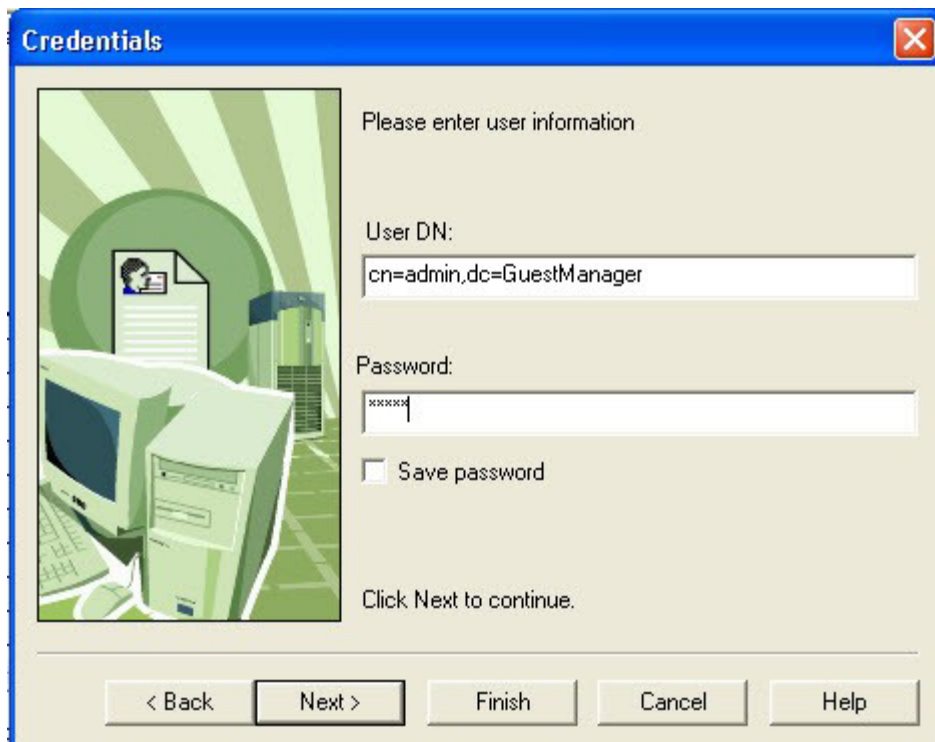
Fetch DN's (only LDAP v.3)

☐ Anonymous bind

Click Next to continue.

< Back Next > Finish Cancel Help

6. Click Next
7. User DN is - cn=admin,dc=GuestManager
8. Password is the password you created when setting up the LDAP FortiConnect.



The 'Credentials' dialog box has a blue title bar with a close button. On the left is an illustration of a computer monitor and tower. The main area contains the text 'Please enter user information'. Below this are two text input fields: 'User DN:' with the value 'cn=admin,dc=GuestManager' and 'Password:' with masked characters 'xxxxx'. A checkbox labeled 'Save password' is unchecked. At the bottom, there are five buttons: '< Back', 'Next >', 'Finish', 'Cancel', and 'Help'. The text 'Click Next to continue.' is located above the 'Next >' button.

Please enter user information

User DN:
cn=admin,dc=GuestManager

Password:
xxxxx

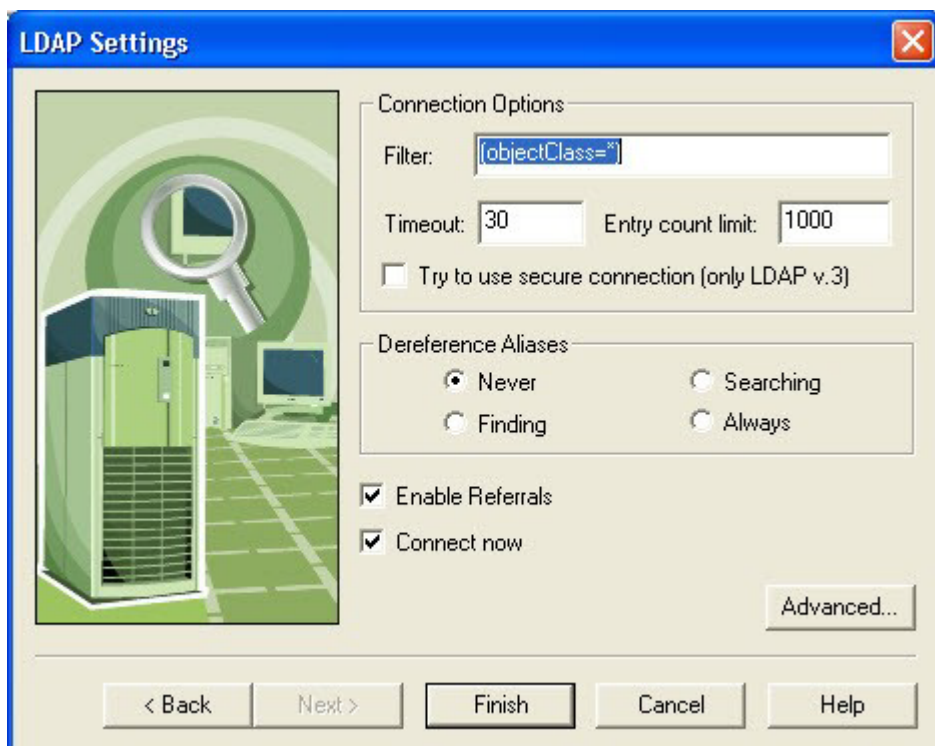
☐ Save password

Click Next to continue.

< Back Next > Finish Cancel Help

9. Click Next

10. Leave the filter as it appears, this will search for all entries.



The 'LDAP Settings' dialog box has a blue title bar with a close button. On the left is an illustration of a server rack with a magnifying glass over it. The main area is divided into sections. 'Connection Options' includes a 'Filter:' field with '(objectClass=*)', 'Timeout:' set to '30', 'Entry count limit:' set to '1000', and an unchecked checkbox 'Try to use secure connection (only LDAP v.3)'. 'Dereference Aliases' has four radio buttons: 'Never' (selected), 'Finding', 'Searching', and 'Always'. Below these are two checked checkboxes: 'Enable Referrals' and 'Connect now'. An 'Advanced...' button is at the bottom right. At the very bottom are five buttons: '< Back', 'Next >', 'Finish', 'Cancel', and 'Help'.

LDAP Settings

Connection Options

Filter: (objectClass=*)

Timeout: 30 Entry count limit: 1000

☐ Try to use secure connection (only LDAP v.3)

Dereference Aliases

☒ Never ☐ Searching
☐ Finding ☐ Always

☒ Enable Referrals
☒ Connect now

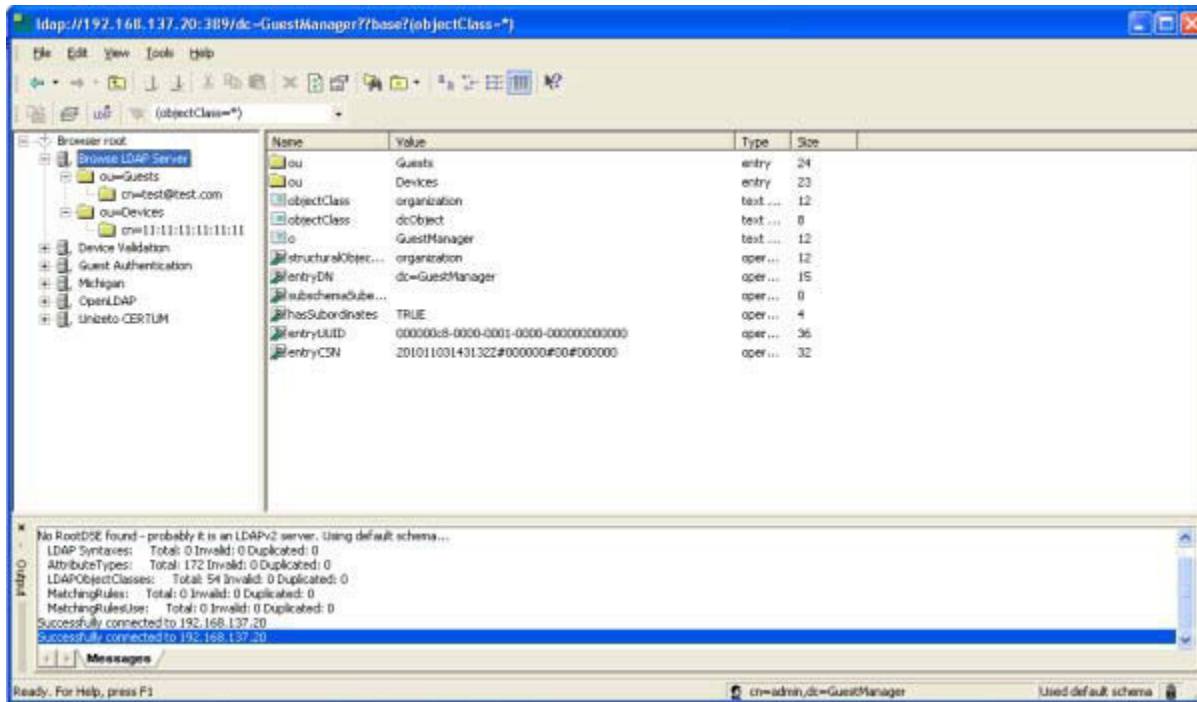
Advanced...

< Back Next > Finish Cancel Help

Browsing the LDAP Database

11. Click Finish

Search results will display everything in the Database under the Browse LDAP Server folder as shown below.

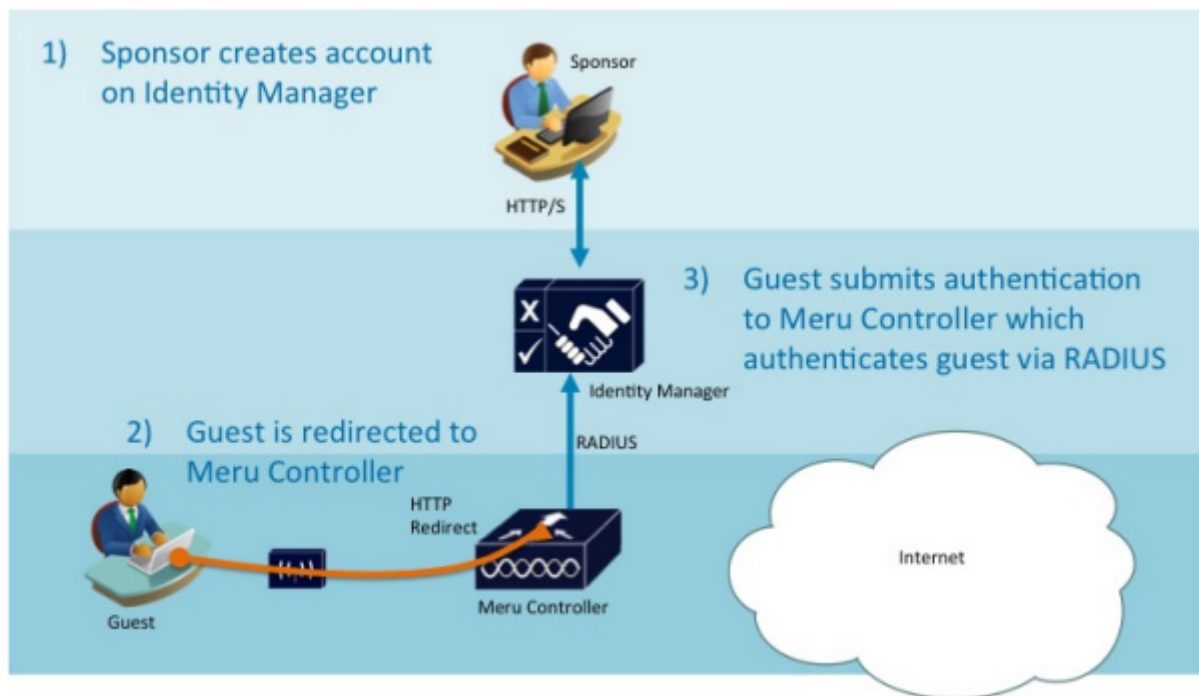


Integrating with a FortiWLC

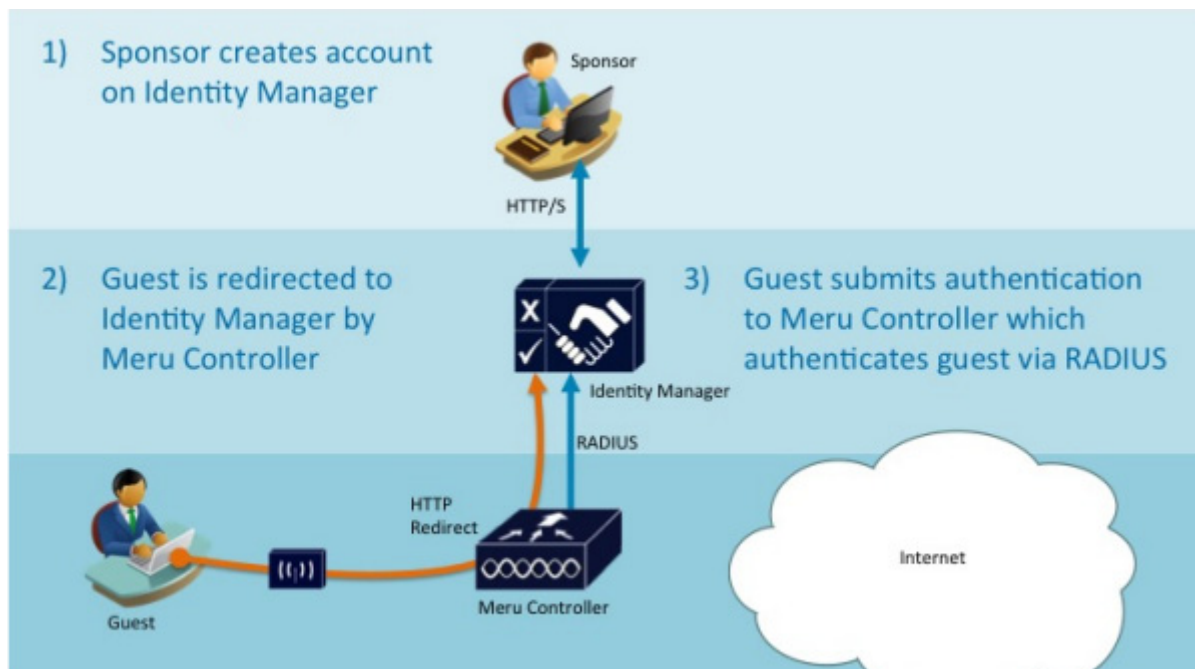
FortiConnect can be integrated with Fortinet Networks Wireless Controllers to provide a fully integrated solution for authenticating, managing and reporting on users accessing the network with web authentication.

There are two different options for FortiConnect integration:

1. Internal Captive Portal on Fortinet Controllers - You can use the integrated portal pages on the Fortinet Controller to provide the portal web pages. users authenticate against the Fortinet Controller which in turn authenticates the user against the FortiConnect using RADIUS.



2. External Captive Portal on FortiConnect - You can host the portal pages directly on the FortiConnect, this provides additional benefits and features such as Self Service, Smart Connect, Password Change, Billing Support and Acceptable Use Pages. This works by having the Fortinet Controller redirect the user to the FortiConnect. The FortiConnect web pages submit the authentication to the Fortinet Controller which then authenticates the user against the FortiConnect using RADIUS.



Baseline Configuration

Prior to configuring the integration the following was carried out using the steps shown in the relevant configuration guides for FortiConnect and Fortinet Configuration Guides.

- Fortinet
 - ⑧ initial setup
 - ⑧ licenses installed
 - ⑧ access points added to the system
 - ⑧ add an ESS profile
- FortiConnect
 - ⑧ initial setup
 - ⑧ licenses installed
 - ⑧ sponsors configured and permitted to create user accounts

This configuration must be performed before moving on with following the instructions in the rest of this chapter.

Adding the Fortinet Controller to FortiConnect

Adding a RADIUS Client to the FortiConnect

The first step is to configure the FortiConnect to allow the Fortinet Controller to authenticate using RADIUS.

1. Login to the admin interface of the FortiConnect at <https://identitymanager/admin>
2. Navigate to Devices > RADIUS Clients
3. Click the Add RADIUS Client button and you will see the screen as shown below

RADIUS Clients

Client | Attributes | SNMP | MAC Authentication | RadSec Authentication

Name:

Device IP Address / Prefix Length:
For example 192.168.1.1/32 or fec0:0001::128

Secret: Confirm:

Type:
If your RADIUS client vendor is not listed please select Generic RADIUS Device

Description:

Change-of-Authorization

Use COA: ☐

Port:

4. Enter the Name that you want to remember the device with.
5. Enter the Device IP Address of the Fortinet Controller. This is the IP address that will be sending RADIUS requests to the FortiConnect.
6. Enter a shared Secret and Confirm it, this value will need to be entered onto the Fortinet Controllers RADIUS setup.
7. Set the Type to Fortinet (Two Options are available, Fortinet SD 5.3 & Earlier and Fortinet SD 6.0 & Later)

Click Save.

Automatically Configuring the Fortinet Controller to authenticate against FortiConnect

8. When you are adding RADIUS for authentication with a Fortinet Controller you will see the tab appear as shown below.

RADIUS Clients

The Meru Connect is using a self-signed SSL certificate, you may get certificate warnings on your clients when they attempt to authenticate

Client | Attributes | SNMP | MAC Authentication | RadSec Authentication | **Automatic Setup**

Meru Connect Address: 192.168.137.20
This hostname is used to redirect guests to the Meru Connect, it should match the SSL certificate on Meru Connect.

Device IP Address: 10.10.1.2

Admin user name: [Redacted]

Admin Password: [Redacted]

Configure RADIUS profiles: ☒

Set Captive Portal RADIUS profiles: ☒

Set Captive Portal External URL: ☒

Configure QoS Rules: ☒

Write changes to startup-config: ☐ This will overwrite your startup-config with the current running-config

Setup Controller

9. Within this tab you can automate several configuration steps between the FortiConnect and the Fortinet Controller. Steps you previously took when setting up the client and SNMP will also be automated once you click on the Setup Controller button :-
- FortiConnect Address - Enter the Address of the FortiConnect
 - Device IP Address - Enter the IP Address of the controller, this is the IP address
 - Admin User Name - Enter the admin user name for the controller
 - Admin Password - Enter the admin password for the controller
 - Configure RADIUS Profiles - Check the box to Configure RADIUS profiles for authentication and account
 - Set Captive portal RADIUS profiles - Check the box to set captive portal RADIUS profiles

- Set Captive portal mode - Check the box to set the captive portal mode to customized
- Configure QoS Rules - Check the box to configure Pre Authentication QoS Rules
- Transfer Pages to Controller - Check the box to transfer portal redirection pages to controller
- Configure SNMP - Check the box to configure SNMP settings (only visible when SNMP has been enabled within the SNMP tab)
- Write changes to startup-config - Check this box to write the current controller running configuration to the startup-config file, this allows config to be retained between reboots.

10. Click on the Setup Controller button to apply the selection confirmation to the controller.

11. Click on the Download portal pages link for manual upload to the RADIUS client

12. Configuration of the settings above do not include configuration of ESS and Security Profile on the Fortinet Controller, the sections below will detail how to do this.

Note: System Director 6.0 & Later - for versions of System Director 6.0 and later we configure the Captive Portal External URL with a redirection URL pointing to the FortiConnect. Also, Automatic Setup no longer requires you to Transfer Custom Portal Pages from the FortiConnect to the controller, Set the Captive Portal Mode to Customized and Set the Captive Portal Authentication Method to Internal as shown in the screenshot below.

Identity Manager Address:
This hostname is used to redirect guests to the Identity Manager, it should match the SSL certificate on Identity Manager.

Device IP Address:

Admin user name:

Admin Password:

Configure RADIUS profiles: ☒

Set Captive Portal RADIUS profiles: ☒

Set Captive Portal External URL: ☒

Configure QoS Rules: ☒

Write changes to startup-config: ☐ This will overwrite your startup-config with the current running-config

Manually Configuring the Fortinet Controller to authenticate against FortiConnect

Adding the FortiConnect as a RADIUS Server

You can manually configure the Fortinet Controller to authenticate against the FortiConnect. The first step is to configure the FortiConnect as a RADIUS server to allow the Fortinet Controller to authenticate users using RADIUS against the FortiConnect.

RADIUS for Authentication

1. Login to the admin interface of the Fortinet Controller
2. Navigate to Configuration > Security > Radius
3. Click Add
4. Enter the RADIUS Profile Name as IDM-Auth
5. Enter a Description
6. Enter the RADIUS IP as the IP address of your FortiConnect
7. Enter the RADIUS Secret to match the value you entered on the FortiConnect.
8. Enter the RADIUS Port as 1812
9. Set the MAC Address Delimiter to Hyphen (-)
10. Enter the Password Type as Shared Key
11. Click OK

RADIUS Profile Table - Add

RADIUS Profile Name	<input type="text" value="IDM-Auth"/>	Enter 1-16 chars., Required
Description	<input type="text" value="Manager Authentication"/>	Enter 0-128 chars.
RADIUS IP	<input type="text" value="10"/> . <input type="text" value="10"/> . <input type="text" value="10"/> . <input type="text" value="200"/>	
RADIUS Secret	<input type="password" value="••••••"/>	
RADIUS Port	<input type="text" value="1812"/>	Valid range: [1024-65535]
MAC Address Delimiter	<input type="text" value="Hyphen (-)"/>	
Password Type	<input type="text" value="Shared Key"/>	

RADIUS for Accounting

1. Navigate to Configuration > Security > Radius
2. Click Add
3. Enter the RADIUS Profile Name as IDM-Acct
4. Enter a Description
5. Enter the RADIUS IP as the IP address of your FortiConnect
6. Enter the RADIUS Secret to match the value you entered on the FortiConnect.
7. Enter the RADIUS Port as 1813
8. Set the MAC Address Delimiter to Hyphen (-)
9. Click OK

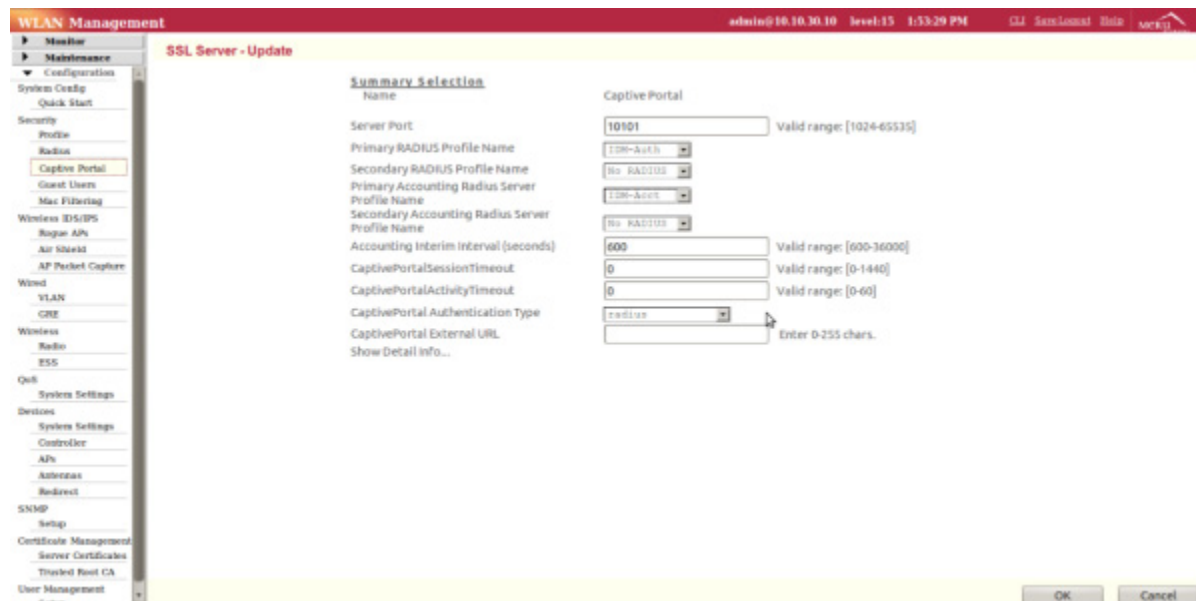
RADIUS Profile Table - Add

RADIUS Profile Name	<input type="text" value="IDM-Acct"/>	Enter 1-16 chars., Required
Description	<input type="text" value="ity Manager Accounting"/>	Enter 0-128 chars.
RADIUS IP	<input type="text" value="10"/> . <input type="text" value="10"/> . <input type="text" value="10"/> . <input type="text" value="200"/>	
RADIUS Secret	<input type="password" value="••••••"/>	
RADIUS Port	<input type="text" value="1812"/>	Valid range: [1024-65535]
MAC Address Delimiter	<input type="text" value="Hyphen (-)"/>	
Password Type	<input type="text" value="Shared Key"/>	

Configure RADIUS Authentication for Captive Portals

Once you have added the FortiConnect as a RADIUS server you need to tell the Fortinet Controller to use these RADIUS servers for web authentication.

1. Navigate to Configuration > Security > Captive Portal
2. Set the Primary RADIUS Profile Name to IDM-Auth
3. Set the Primary Accounting Radius Server Profile Name to IDM-Acct
4. Set the Captive Portal Authentication Type to radius
5. Click OK



Configure the Security Profile for Captive Portal

To enable the captive portal you need to change the security profile for the ESS profile that you want to use for user access.

In the following configuration example we will modify the default Security Profile, and create a new ESS profile which uses it.

Configure the Security Profile

1. Navigate to Configuration > Security > Profile
2. Check the default Security Profile and click Settings
3. Change the Captive Portal setting to WebAuth
4. Set the Captive Portal Authentication Method to internal
5. Click Ok.

Security Profile Table - Update

Summary Selection

Profile Name	idm
L2 Modes Allowed	<input checked="" type="checkbox"/> Clear <input type="checkbox"/> 802.1x <input type="checkbox"/> Static WEP keys <input type="checkbox"/> WPA <input type="checkbox"/> WPA PSK <input type="checkbox"/> WPA2 <input type="checkbox"/> WPA2 PSK <input type="checkbox"/> MIXED <input type="checkbox"/> MIXED_PSK
Data Encrypt	<input type="checkbox"/> WEP64 <input type="checkbox"/> WEP128 <input type="checkbox"/> TKIP <input type="checkbox"/> CCMP-AES <input type="checkbox"/> CCMP/TKIP <input type="checkbox"/> Clear
Primary RADIUS Profile Name	No RADIUS ▼
Secondary RADIUS Profile Name	No RADIUS ▼
WEP Key (Alphanumeric/Hexadecimal)	
Static WEP Key Index	1 Valid range: [1-4]
Re-Key Period (seconds)	0 Valid range: [0-65535]
Captive Portal	WebAuth ▼
Captive Portal Authentication Method	internal ▼
802.1X Network Initiation	Off ▼

Create an ESS

1. Navigate to Configuration > Wireless > ESS
2. Add a new ESS by clicking the Add button
3. Set the ESS Profile Name and SSID to guestnetwork
4. Set the Security Profile Name to default
5. Click Add

ESS Profile - Add

ESS Profile Name	<input type="text" value="guestnetwork"/>	Enter 1-32 chars., R
Enable/Disable	<input type="button" value="Enable"/> ▼	
SSID	<input type="text" value="guestnetwork"/>	Enter 0-32 chars.
Security Profile Name	<input type="text" value="idm"/> ▼	
Primary RADIUS Accounting Server	<input type="button" value="No RADIUS"/> ▼	
Secondary RADIUS Accounting Server	<input type="button" value="No RADIUS"/> ▼	
Accounting Interim Interval (seconds)	<input type="text" value="3600"/>	Valid range: [600-3600]
Beacon Interval (msec)	<input type="text" value="100"/>	Valid range: [20-1000]
SSID Broadcast	<input type="button" value="On"/> ▼	
Bridging	<input type="checkbox"/> AirFortress <input type="checkbox"/> IPV6 <input type="checkbox"/> AppleTalk	
New AP's Join ESS	<input type="button" value="On"/> ▼	

You should now be able to authenticate a user with web authentication against the FortiConnect.

SNMP Integration

For audit purposes you will want to know the IP address assigned to each of your users. The IP address of the user is also required for correlating the syslog messages from firewalls.

SNMP needs to be setup to obtain the IP address of the user from the Fortinet Controller as it isn't sent in the RADIUS Accounting messages (before System Director Release 5.1). When a user authenticates the FortiConnect receives the MAC address of user from the Fortinet Controller in the calling-station-id field. The FortiConnect then contacts the Fortinet Controller using SNMP to find the IP address for this device and fills in the Framed-IP-Address details in the RADIUS Accounting database.

Configuring SNMP on the Fortinet Controller

The best way of setting up SNMP on the Fortinet Controller is to use the command line. This enables you to setup SNMP version 3 which supports authentication and encryption. SNMPv3 is also more efficient in terms of communication than SNMPv1. Only SNMP version 1 can be setup from the web interface on the Fortinet Controller.

To setup SNMP on the controller perform the following steps:

Connect to the command line of the controller, using the console port, telnet or ssh. Login as the admin user.

1. Enter configuration mode by entering the following:

```
meru-mc1500(15)# configure terminal
```

2. Enter the SNMP global settings:

```
meru-mc1500(15)(config)# snmp-server contact admin@merunetworks.com
```

```
meru-mc1500(15)(config)# snmp-server description Meru_MC-1500_Controller
```

```
meru-mc1500(15)(config)# snmp-server location Manchester
```

3. Configure an SNMPv3 User:

```
meru-mc1500(15)(config)# snmpv3-user identitymanager
```

4. Setup the authentication and privacy protocols and passwords

```
meru-mc1500(15)(config-snmpv3-user)# auth-protocol md5-auth
```

```
meru-mc1500(15)(config-snmpv3-user)# auth-key 1Dent1ty
```

```
meru-mc1500(15)(config-snmpv3-user)# priv-protocol des-priv
```

```
meru-mc1500(15)(config-snmpv3-user)# priv-key 1Dent1ty
```

5. Setup the IP address of the FortiConnect that can connect to the Controller using SNMP

```
meru-mc1500(15)(config-snmpv3-user)# target-ip-address [FortiConnect IP address]
```

6. Finish configuration.

```
meru-mc1500(15)(config-snmpv3-user)# end
```

7. Lastly you need to start SNMP running on the controller:

```
meru-mc1500(15)# snmp start
```

8. You can verify that the snmp service is running by entering `snmp status`

SNMP is now configured correctly on the controller.

Configuring SNMP on the FortiConnect

To enable the FortiConnect to use SNMP to fill in missing Framed-IP-Address for RADIUS clients you need to enable SNMP on each RADIUS client.

Perform the following steps to enable SNMP for the FortWLC:

1. From the FortiConnect Administration interface navigate to Devices > RADIUS Clients
2. Select the Fortinet Controller from the list of devices.
3. Select the SNMP tab

RADIUS Clients

Client | Attributes | **SNMP** | MAC Authentication | RadSec Authentication | Automatic Setup

SNMP is used for recording the Framed-IP-Address of the guest when the RADIUS client does not set this in RADIUS accounting messages. You do not need to enable this if the device sets it correctly.

Enable: ☒

Alternative SNMP device IP Address: If the RADIUS Client doesn't support SNMP access to the ARP table, query this device instead

Version: **V3** V2: & V3 perform better than V1

Read Community:

Authentication Protocol: **MD5**

Authentication Username:

Authentication Passphrase: Confirm:

Privacy Protocol: **DES**

Privacy Passphrase: Confirm:

Security Type: **Authentication**

Save **Cancel**

4. Check the Enable checkbox
5. Set the Version to V3
6. Select the Authentication Protocol as MD5
7. Enter the Authentication Username as identitymanager
8. Set the Authentication Passphrase to 1Dent1ty and Confirm it

9. Set the Privacy Protocol to DES
10. Set the Privacy Passphrase to 1Dent1ty and Confirm it
11. Set the Security Type to Encryption
12. Click Save.

Now that you have enabled SNMP every minute after a user has logged in the FortiConnect will obtain their IP address from the Fortinet Controller and record it in the RADIUS Accounting record.

Using FortiConnects Portals with Meru Controllers

Allowing access to the FortiConnect

To allow traffic to reach the FortiConnect so that it can be used as the external portal you need to have the Personal Enforcement Firewall feature enabled on the controller and then setup QoS rules to allow the traffic through

Controller Qos Rules

Configure the 2 QOS rules one for incoming and other for outgoing traffic to the FortiConnect. At this point you should have the FortiConnects system's Ip address and the corresponding Port number is 443 for HTTPS.

To add the QOS Rules

1. Click on the Configuration Panel-->QOS-->System Settings.
2. Click on QOS and Firewall Rules Tab as shown in the figure below.
3. Click on the ADD button below as shown in the figure below

QoS and Firewall Rules (18 entries)

Global Quality-of-Service Parameters		QoS and Firewall Rules			QoS Codec Rules		
<input type="checkbox"/>	ID	Destination IP	Destination Netmask	Destination Port	Source IP	Source Netmask	Source Port
<input type="checkbox"/>	3	0.0.0.0	0.0.0.0	5060	0.0.0.0	0.0.0.0	0
<input type="checkbox"/>	4	0.0.0.0	0.0.0.0	0	0.0.0.0	0.0.0.0	5060
<input type="checkbox"/>	7	0.0.0.0	0.0.0.0	5200	0.0.0.0	0.0.0.0	0
<input type="checkbox"/>	8	0.0.0.0	0.0.0.0	0	0.0.0.0	0.0.0.0	5200
<input type="checkbox"/>	119	0.0.0.0	0.0.0.0	0	0.0.0.0	0.0.0.0	0
<input type="checkbox"/>	10	10.0.0.0	255.0.0.0	0	192.168.37.0	255.255.255.0	0
<input type="checkbox"/>	11	172.27.0.0	255.255.192.0	0	192.168.37.0	255.255.255.0	0
<input type="checkbox"/>	13	172.26.0.0	255.255.192.0	0	192.168.37.0	255.255.255.0	0
<input type="checkbox"/>	14	172.27.0.0	255.255.192.0	0	192.168.37.0	255.255.255.0	0
<input type="checkbox"/>	15	172.26.0.0	255.255.192.0	0	192.168.37.0	255.255.255.0	0
<input type="checkbox"/>	16	0.0.0.0	0.0.0.0	4500	0.0.0.0	0.0.0.0	4500
<input type="checkbox"/>	27	10.0.0.10	255.255.255.255	0	192.168.37.0	255.255.255.0	0
<input type="checkbox"/>	26	10.0.0.0	255.0.0.0	0	192.168.37.0	255.255.255.0	0
<input type="checkbox"/>	28	192.168.34.0	255.255.255.0	0	0.0.0.0	0.0.0.0	0
<input type="checkbox"/>	1	0.0.0.0	0.0.0.0	1720	0.0.0.0	0.0.0.0	0
<input type="checkbox"/>	2	0.0.0.0	0.0.0.0	0	0.0.0.0	0.0.0.0	1720
<input type="checkbox"/>	30	192.168.34.20	255.255.255.255	443	0.0.0.0	0.0.0.0	0
<input type="checkbox"/>	31	0.0.0.0	0.0.0.0	0	192.168.34.20	255.255.255.255	443

Add a QoS Rule for Destination Traffic

Once you have clicked the Add button, you will see the screen below.

QoS and Firewall Rules - Add

ID	<input type="text"/>	Valid range: [0-600]
Destination IP	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>	
Destination Netmask	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>	
Destination Port	<input type="text"/>	Valid range: [0-655]
Source IP	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>	
Source Netmask	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>	
Source Port	<input type="text"/>	Valid range: [0-655]
Network Protocol	<input type="text"/>	Valid range: [0-255]
Firewall Filter ID	<input type="text"/>	Enter 0-16 chars.
Packet minimum length	<input type="text"/>	Valid range: [0-150]
Packet maximum length	<input type="text"/>	Valid range: [0-150]
QoS Protocol	<input type="text" value="SIP"/>	
Average Packet Rate	<input type="text"/>	Valid range: [0-200]
Action	<input type="text" value="FORWARD"/>	
Drop Policy	<input type="text" value="Tail"/>	
Token Bucket Rate	<input type="text"/> <input checked="" type="checkbox"/> Kbps <input type="checkbox"/> Mbps	
Priority	<input type="text"/>	Valid range: [0-8]
Traffic Control	<input type="text" value="Off"/>	
DiffServ Codepoint	<input type="text" value="DiffServ Disabled"/>	

Configure the following with



1. ID should be a unique number not used for any other rule.
2. Destination IP address should be the FortiConnects IP address, The Net Mask should be 255.255.255.255. Select the check box in the Match column next to it.
3. Set the Destination port to 443. Select the check box in the Match column next to it.
4. Set the Network Protocol to 6. Select the check box in the Match column next to it.
5. Enter Firewall Filter ID ensuring there are no spaces (use a name such as IdentityManager) and select the check box in the Match column next to it.
6. Select the QOS protocol as other.
7. Once done click on OK

Similarly Add a QOS Rule for Source Traffic

To Configure the Source Rule follow the steps below:

1. Click on ADD
1. ID should be a unique number not used for any other rule.
2. Source IP address should be the FortiConnects IP address, The Net Mask should be 255.255.255.255. Select the check box in the Match column next to it.
3. Set the Source port to 443. Select the check box in the Match column next to it.
4. Set the Network Protocol to 6, Select the check box in the Match column next to it.
5. Enter Firewall Filter ID (give same name as given above for destination traffic) and select the check box in the Match column next to it.
6. Select the QOS protocol as others.
7. Once done click on OK

Once the above steps are completed you will get a screen as shown below

	30	192.168.34.20	255.255.255.255	443	0.0.0.0	0.0.0.0	0	6
	31	0.0.0.0	0.0.0.0	0	192.168.34.20	255.255.255.255	443	6

Security Profile

To configure a security profile for the FortiConnect portal authentication follow the following steps: click Configuration > Security > Profile. Then you will get a Security profile table with list security profiles if configured. Click on ADD as shown in the figure below

Security Profile Table - Add

Security Profile Name	<input style="width: 90%;" type="text" value="idm-security"/> <small>Enter 1-32 chars., R</small>
L2 Modes Allowed	<input checked="" type="checkbox"/> Clear <input type="checkbox"/> 802.1x <input type="checkbox"/> Static WEP keys <input type="checkbox"/> WPA <input type="checkbox"/> WPA PSK <input type="checkbox"/> WPA2 <input type="checkbox"/> WPA2 PSK <input type="checkbox"/> MIXED <input type="checkbox"/> MIXED_PSK
Data Encrypt	<input type="checkbox"/> WEP64 <input type="checkbox"/> WEP128 <input type="checkbox"/> TKIP <input type="checkbox"/> CCMP-AES <input type="checkbox"/> CCMP/TKIP <input type="checkbox"/> Clear
Primary RADIUS Profile Name	<div style="border: 1px solid #ccc; padding: 2px; display: inline-block;">No RADIUS</div>
Secondary RADIUS Profile Name	<div style="border: 1px solid #ccc; padding: 2px; display: inline-block;">No RADIUS</div>
WEP Key (Alphanumeric/Hexadecimal)	<div style="border: 1px solid #ccc; height: 20px; width: 100%;"></div>
Static WEP Key Index	<div style="border: 1px solid #ccc; padding: 2px; display: inline-block;">1</div> <small>Valid range: [1-4]</small>
Re-Key Period (seconds)	<div style="border: 1px solid #ccc; padding: 2px; display: inline-block;">0</div> <small>Valid range: [0-65535]</small>
Captive Portal	<div style="border: 1px solid #ccc; padding: 2px; display: inline-block;">WebAuth</div>
Captive Portal Authentication Method	<div style="border: 1px solid #ccc; padding: 2px; display: inline-block;">internal</div>
802.1X Network Initiation	<div style="border: 1px solid #ccc; padding: 2px; display: inline-block;">On</div>

Configure a security profile for the External Captive Portal as shown below,

1. Enter a name to the Security Profile
2. Select Captive Portal to WebAuth
3. Select Captive Portal Authentication method to internal
4. Set the Passthrough Firewall Filter ID to the same name as the Firewall Filter ID defined in the QOS rule.

Uploading Custom Portal Pages

This section details how to upload the custom portal pages to the FortiWLC.

1. To upload the pages Manually, go to Devices --> RADIUS Clients and click on the Automatic Setup Tab as shown below.

Uploading Custom Portal Pages

The screenshot shows the 'Automatic Setup' tab in the FortiConnect configuration interface. The 'RadSec Authentication' sub-tab is selected. The form contains the following fields and options:

- Identity Manager Address:** 192.168.137.20. A note below states: 'This hostname is used to redirect guests to the Identity Manager, it should match the SSL certificate on Identity Manager.'
- Device IP Address:** 10.10.10.1
- Admin user name:** (empty text box)
- Admin Password:** (empty password box)
- Configure RADIUS profiles:** ☒
- Set Captive Portal RADIUS profiles:** ☒
- Set Captive portal mode:** ☒
- Configure QoS Rules:** ☒
- Transfer pages to controller:** ☒
- Write changes to startup-config:** ☐ This will overwrite your startup-config with the current running-config

At the bottom, there is a 'Setup Controller' button and a link: [Download portal pages](#) for manual upload to the RADIUS client.

2. Click on the Download Portal Pages link and this will download a .zip file containing the pages which you can then manually upload to the controller.
3. To manually upload go to Maintenance-->Captive Portal on the FortWLC and click on the Import File link.

Import File

Step 1

Select a File

- Clicking the **Browse...** button allows to choose the file you wish to Import.
- Only Files with the extensions: **.html, .gif, .jpg, .png, .bmp, .css, .js** are allowed.
- The extension defines the content of the file to be imported.

Step 2

Import the selected File

- Click **Import File** button to start the Import Process.
-

4. Click on Choose File and select the pages that are in the .zip file.
5. Then browse to your FortWLC and select Maintenance-->Captive Portal and click on the Customization link as shown below.

Captive Portal Customization

Step 1

Select a Mode

Captive Portal has 2 Modes of Operation: **Default** and **Customized**

- Default Mode: HTML documents are generated at installation and the user cannot change the
- Customized Mode: The login page and other GUI elements are served from a custom directory
 - Get Files Downloads the HTML pages which can be customized(**.html**).
 - Delete Files Erase the custom directory(**.gif, .jpg, .png, .bmp, .css, .js, .html, .pl**).
 - Restore Default The custom directory is restored to the installation content(**.html**).
 - To test the customization:
 1. Import the customized file(s)(**.gif, .jpg, .png, .bmp, .css, .js, .html, .pl**)
 2. Type the test URL `https://controller/vpn/customfile.html`
 3. See Online Help for more information

Step 2

Change the Mode

6. Set the Mode Selection to Customized and click "Change Mode"

User Account Notification

When a User account is created, the details of the account need to be passed from the sponsor to the User. The FortiConnect provides a number of ways to do this:

- Manually reading the details to the User from the screen.
- Printing the details out on paper.
- Sending the details in an email.
- Sending the details as an SMS text message.

Sponsors always have the option of reading and printing out User account details to Users. Email and SMS text message notification require email servers to be configured, but can be configured based upon policy.

Note: Email and SMS User account notification policies need to be configured globally, then enabled per user group for individual sponsor permissions.

This chapter describes the following:

- Configuring Email Notification
- Configuring SMS Notification
- Print Notification

Configuring Email Notification

The following steps describe how to configure email settings for the FortiConnect to correctly deliver User account details via email.

1. From the administration interface, select Devices > Email Settings from the left hand menu

Email Settings

SMTP Settings

Enable Email: ☒

Send Emails From:

SMTP Server:

SMTP Encryption: TLS If using SSL or TLS certificates are uploaded in Server > SSL Settings > Trusted CA Certificates

SMTP Port:

SMTP Authentication: Plain

SMTP Username:

SMTP Password: Confirm:

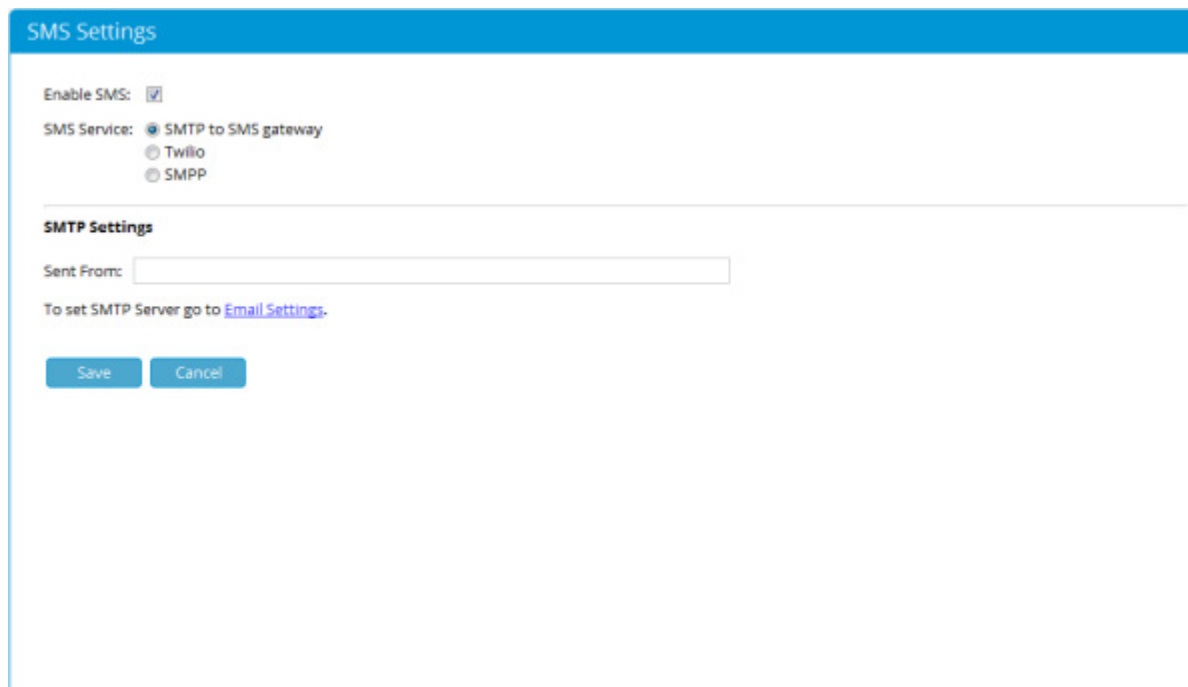
2. In the Email Settings page as shown above, check the Enable Email option to enable email functionality globally for the FortiConnect.
3. For SMTP Server, type the IP address of the outbound SMTP server to which you need to deliver email. If you enter localhost, or leave this field empty, the FortiConnect attempts to deliver the email directly to the User's SMTP server.
4. In the Sent From field, type the email address from which you want User notification emails to be sent (for example, host@company.com).
5. From the SMTP Encryption drop down box, select whether SSL or TLS encryption is required. Certificates can be uploaded in the Server -->SSL Settings section.
6. From the SMTP Authentication drop down box you can select from three different types of authentication modes, select from Plain, Login or CRAM-MDS and enter the SMTP username and password details where required.
7. Click the Save Settings button.
8. Once this has been set up, you can perform an SMTP test by entering an email address in the Send test email to field.

Note: Refer to Editing the Email Template for additional details.

Configuring SMS Notification

Short Message Service (SMS) is delivered through an SMS gateway service that supports SMTP (Simple Mail Transport Protocol) delivery. You need to have an internal SMS gateway service or subscribe to an external service to be able to deliver User details via SMS.

1. From the administration interface, select Devices > SMS Settings from the left hand menu.



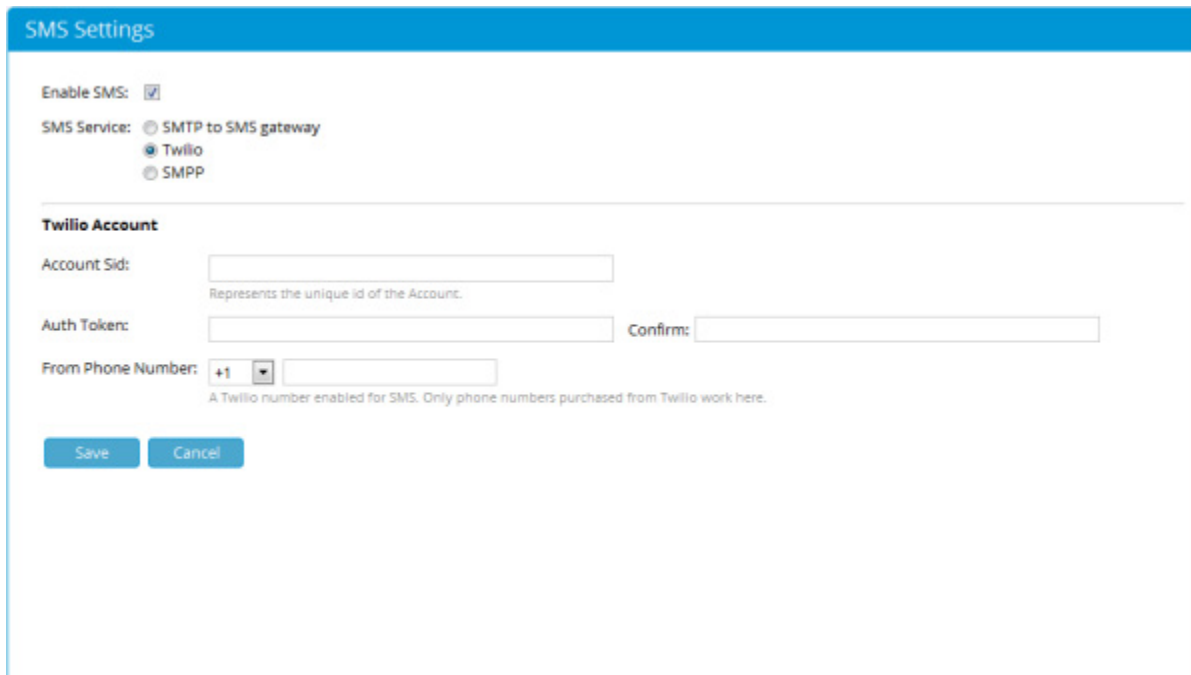
The screenshot shows the 'SMS Settings' configuration page. At the top, there is a blue header bar with the text 'SMS Settings'. Below this, the 'Enable SMS' checkbox is checked. Under 'SMS Service', three radio buttons are visible: 'SMTP to SMS gateway' (selected), 'Twilio', and 'SMPP'. A horizontal line separates the service selection from the 'SMTP Settings' section. In the 'SMTP Settings' section, there is a 'Sent From' text input field. Below the input field, a note states 'To set SMTP Server go to [Email Settings](#)'. At the bottom of the form, there are two buttons: 'Save' and 'Cancel'.

2. In the SMS Settings page as shown above, check the Enable SMS checkbox to globally enable SMS on the FortiConnect.
3. SMTP to SMS Gateway - Check this for SMTP to SMS gateway. SMS requires an SMTP server to deliver the email to the SMS gateway. Click on the Email Settings link to configure the SMTP Server as described in the Configuring Email Notification section.
4. Twilio - Check this to send SMS using Twilio.
5. SMPP- Check this to send using SMPP.
6. In the Sent From field, type the sending email address for the email to be sent to the SMS gateway.

7. Click Save Settings.
8. Once this has been set up, you can perform an SMS test by entering a destination in the Destination field.

Note: FortiConnect supports Twilio and SMPP, see below on how to set this up.

9. Twilio - A Twilio API account along with a Twilio enabled phone number would be required to configure with the FortiConnect, enter the relevant details in the screen below.



The screenshot shows the 'SMS Settings' configuration page. At the top, there's a blue header with the text 'SMS Settings'. Below the header, the 'Enable SMS' checkbox is checked. Under 'SMS Service', three radio buttons are present: 'SMTP to SMS gateway', 'Twilio' (which is selected), and 'SMPP'. A horizontal line separates this section from the 'Twilio Account' section below. In the 'Twilio Account' section, there are four input fields: 'Account Sid' (with a placeholder text 'Represents the unique id of the Account.'), 'Auth Token' (with a 'Confirm:' label next to it), and 'From Phone Number' (which includes a dropdown menu showing '+1' and a placeholder text 'A Twilio number enabled for SMS. Only phone numbers purchased from Twilio work here.'). At the bottom of the form, there are two buttons: 'Save' and 'Cancel'.

10. SMPP - (Short Message Peer to Peer) An SMPP API account would be required from the SMSC (Short Message Service Centre) to configure with FortiConnect as shown below.

SMS Settings

Enable SMS: ☒

SMS Service: ☐ SMTP to SMS gateway
☐ Twilio
☒ SMPP

SMSC Settings

Host:

Port:

System Id:

Password: Confirm:

System Type:

An optional login parameter that should be set only if required by the SMSC

11. Click on Save once you have completed entering all the required details.

Note: Depending on how details are routed to the SMS provider, you need to customize the SMS portion of the User Interface template to include the User's mobile phone number in the correct format for your SMS gateway. See Editing the SMS Template for details.

Print Notification

Print notification is configured as described in Editing the Print Template.

User Activity Logging

User Activity Logging provides the ability for the FortiConnect to receive syslog information from network devices such as Firewalls, Proxy Servers and Routers. This information can provide details on all the connections that a User has made and Layer 7 information such as URLs accessed, depending on the network device.

User Activity Logging relies on knowing the IP address for each User as they authenticate to the network. The FortiConnect receives this information from RADIUS accounting, so you need to configure the network device that the user authenticates through to send this information. Commonly, this is the Wireless LAN Controller or NAC Appliance. Refer to the information in, “Configuring RADIUS Clients” for details on adding these devices as a RADIUS client.

Note: User Activity Logging relies on correlating the syslog information with the IP Address received from RADIUS accounting. This means that it will not work if you use a deployment method where the User’s IP address changes after authentication and no additional RADIUS accounting messages are sent.

Once the FortiConnect has the IP Address of each of the Users, then it needs to receive syslog information from the network devices. You should configure each of your network devices to send syslog to UDP port 514 on the FortiConnect. The FortiConnect then processes the syslog information and correlates it against each User. This correlation enables you to view the User’s activity on the User activity log details page for each User as described in Reporting on Users.

User Activity is correlated into individual files that are stored on the disk of the appliance. The appliance can store log files until less than 30% disk space remains; it then either deletes the oldest log files or archives the log files to an external FTP server as described in Configuring

Syslog Monitoring Settings. In addition if archiving is configured, logs are archived every hour to the external FTP server.

Configuring Syslog Monitoring Settings

Archiving of logs to an FTP server provides the ability to store logs for long periods of time, and also provides the ability to back them up.

When viewing the logs through the sponsor interface, the FortiConnect automatically searches for logs on the archive server and displays them in the report for you.

1. From the administration interface, select Devices > Syslog Monitoring from the left hand menu as shown below.

Configuring Syslog Monitoring Settings

Syslog Monitoring

Old Log Files:

Server:

Port:

Directory:

Username:

Password: Confirm:

2. To delete local log files when disk space is low, select Delete oldest local log files when disk space is low and click on save.

Syslog Monitoring

Old Log Files:

Server:

Port:

Directory:

Username:

Password: Confirm:

Passive Mode: ☐

3. To archive logs to an FTP Server select the Archive to FTP Server from the drop down menu and enter the relevant details
 - Server - Server name or IP address
 - Port - Port of the FTP Server
 - Directory - Directory of the FTP server you wish files to be stored in.
 - Username - Username of the account that has the ability to log onto the FTP server
 - Password - Password of the account that has the ability to log onto the FTP server
 - Passive Mode - check box if you wish to use passive mode

Click the Save Button when complete

The screenshot shows a web interface titled "Syslog Monitoring". Under the "Old Log Files:" label, a dropdown menu is set to "Archive to SFTP Server". Below this are several input fields: "Server:" (empty), "Port:" (containing "22"), "Directory:" (empty), "Username:" (empty), "Password:" (empty), and "Confirm:" (empty). At the bottom of the form are two buttons: "Save" and "Cancel".

4. To archive logs to an SFTP Server select the Archive to SFTP Server from the drop down menu and enter the relevant details.
 - Server - Server name or IP address
 - Port - Port of the SFTP Server
 - Directory - Directory of the SFTP server you wish files to be stored in.
 - Username - Username of the account that has the ability to log onto the SFTP server
 - Password - Password of the account that has the ability to log onto the SFTP server
 - Passive Mode - check box if you wish to use passive mode.

Click on the Save Button when complete

User Activity Logging with Replication Enabled

If you have a Cluster of FortiConnects replicating database information for resilience, then the User activity logs are not replicated between each box.

However, if you view the report in the Sponsor interface, the FortiConnect contacts the replication box and retrieves the logs from there. It then displays all logs in a consolidated view. This enables you to have some network devices send syslog to one FortiConnect and some to another, but then view all the results through a single interface.

Each FortiConnect retrieves the logs from the other FortiConnect in the replication pair securely over HTTPS. Each FortiConnect must trust the certificate of the other FortiConnect so that the retrieval can occur properly. To enable this, ensure that the root CA certificate for the other FortiConnect is uploaded as described in [Uploading Certificate Files](#).

Customizing the Application

This chapter describes the following

- User Interface Templates
- Adding a User Interface Template
- Editing a User Interface Template
- Deleting a Template
- Setting the Default Interface Mapping
- Setting User Default Redirection
- Session Time outs
- Login Page Message

User Interface Templates

FortiConnect allows you to customize the sponsor user interface text and User notification text using User Interface Templates. You can:

- Change the labels for the sponsor interface.
- Provide different instructions for users.
- Change the default Acceptable Use Policy.
- Create a translated template to provide the sponsor interface and User instructions in another language altogether.

FortiConnect provides a several template's (in English) that can be used as is without any further modification. If you want to change the default presentation for sponsors and Users, you can add one or multiple templates that you can store separately on the FortiConnect and modify as desired.

Typically, you create a customized template when you need to modify the account details and instructions that are provided to the User, such as the Acceptable Usage Policy. FortiConnect provides Print, Email, and SMS templates that allow you to customize the information that is printed, emailed, or text messaged to Users.

If you are customizing the interface for another language, create a new template for the language and edit all pages with the translated text.

Once your user interface template is configured, you need to set the default template mapping so

that the FortiConnect starts using the correct template. Once a sponsor has authenticated, the sponsor can choose a different template to use and save it under My Settings > Preferences > Language Template in the sponsor interface. This enables each sponsor to have the application displayed in a different template or language.

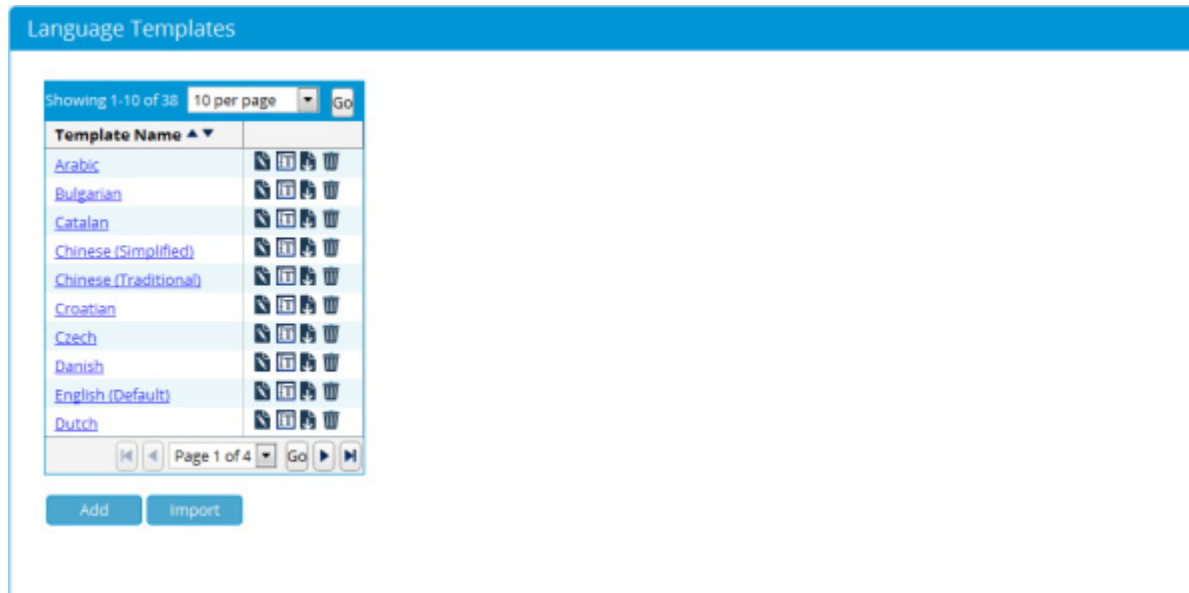
Note: You can set the default user interface template globally for the FortiConnect sponsor and User interfaces under User Interfaces > User Defaults.

TIP - When customizing, it is a good idea to open the sponsor interface in a second browser for reference. This allows you to view how the configuration tabs map to the actual sponsor interface pages. You can bring up the sponsor interface by entering the FortiConnect IP address without the “/admin” as the URL, for example, `http://<meru_connect_ip_address>` or `https://<meru_connect_ip_address>`. The sponsor must logout and login again to view the changes.

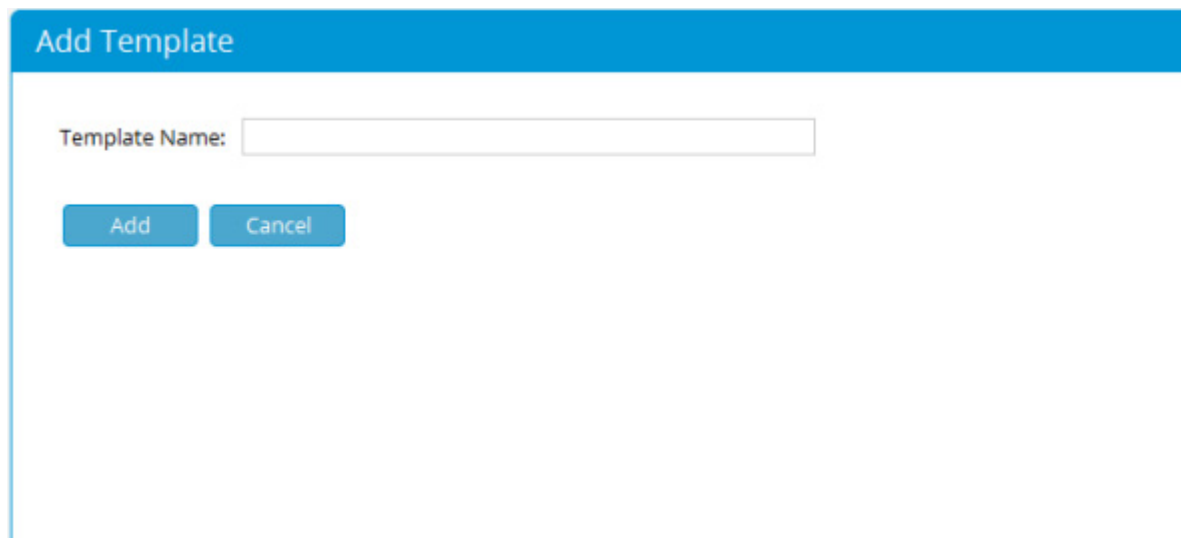
Adding a User Interface Template

When you add a new template, it is automatically based on the default template to facilitate editing.

1. From the administration interface, select Sponsor Portal > Language Templates from the left hand menu.
2. On the User Interface Templates page as shown below, click the Add Template button.



3. In the Add New Template page as shown below, type a Template Name. This can be any descriptive text to identify the template later from the User Interface Templates list as shown above.



The screenshot shows a modal dialog box titled "Add Template". It has a blue header bar with the title. Below the header, there is a label "Template Name:" followed by a text input field. At the bottom of the dialog, there are two buttons: "Add" and "Cancel".

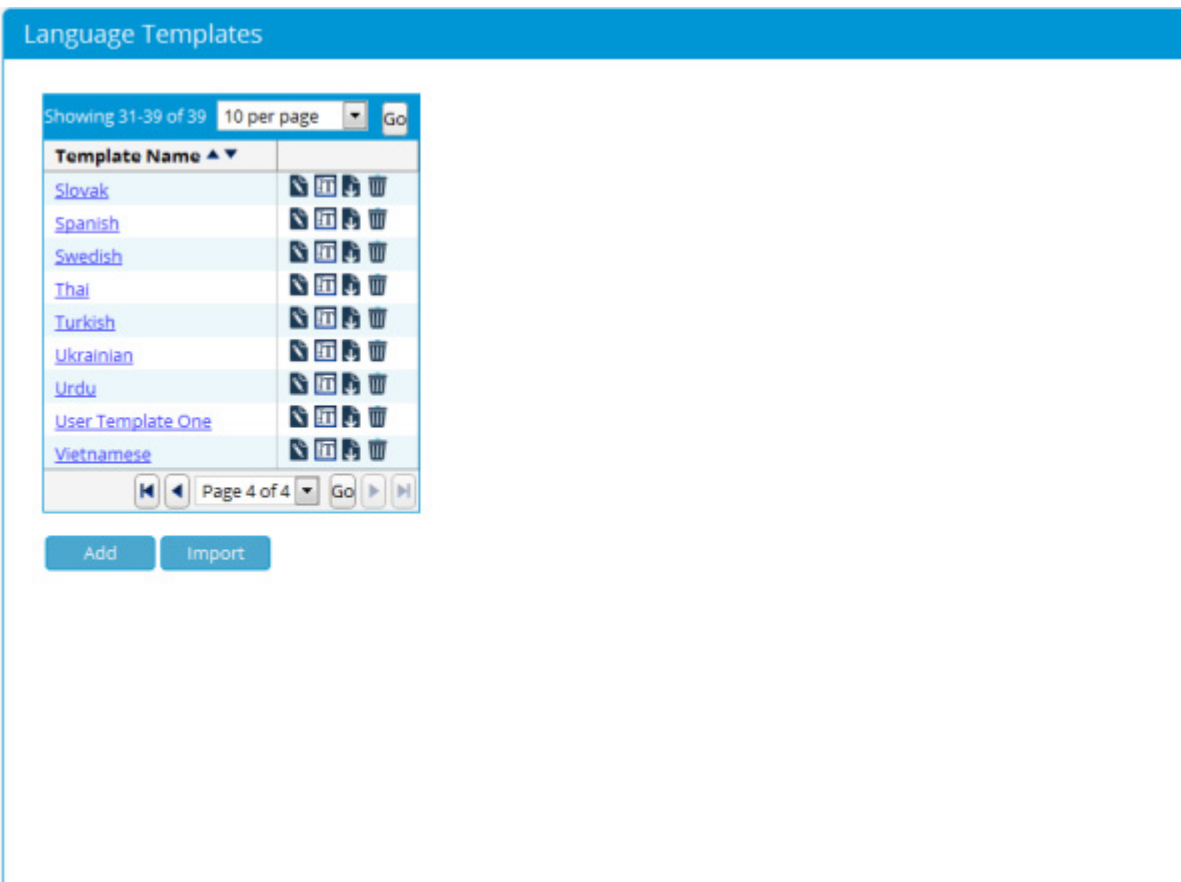
4. Click the Add Template button.

The Edit User Interface Template page for the new template is displayed, initially, with all details copied from the default template. If you only need to make small changes, this allows you not to have to retype all the entries.

5. Modify these settings as desired, as described in Editing a User Interface Template.
6. FortiConnect also allows you to Import a template, this can be done by clicking on the Import Template button.

Editing a User Interface Template

1. From the administration interface, select Sponsor Portal > Language Templates from the left hand menu.



2. From the User Interface Templates list as shown above, click the underlined name of the template you wish to edit.
3. The Edit Home Page for the template is displayed as shown below.

Language Templates: User Template One

Home Menu Reporting Notification Sponsor Settings Guest Accounts Device Accounts Event Codes Common Getting Started Timezones Phone Codes

About: About

Application Title: Meru Connect

Login: Login

Logout: Logout

Username: Username

Password: Password

Version: Version

Serial Number: Serial Number

Logged Out: You are logged out

Not Logged In: Not logged in

Username or Password required: You must enter a username and password

Username or Password invalid: Your username or password is invalid

Save Cancel

4. Click the menu tabs at the top of the page to select any of the sponsor page settings that you want to edit.
5. Make any changes to the fields and click the Save button. Some example edits are described in the following sections:
 - Editing the Guest Print Template
 - Editing the Guest Email Template
 - Editing the Guest SMS Template

Note: The Upload Logo feature allows upload an image with maximum height of 75 pixels and maximum width of 150 pixels. The image can be in .png, .jpg, or .gif format.

Editing the Guest Print Template

The Guest Print Template page contains the User account details that the sponsor can bring up in a browser to print out for handing to the User after the account is created. The page is configured in HTML and can be fully customized.

TIP - Navigating to Account Management > Manage Accounts on the sponsor interface and clicking the Print button next to the User account entry brings up the output of the Print Template for printing.

1. Go to Sponsor Portal > Language Templates and click the underlined name of the template you wish to edit in the Templates list.
2. Under Edit Home Page, click the Notification tab to bring up the Edit Notification Page as shown below.
3. From the Select Template for dropdown menu, choose Guest Print Template and click the Show button.

Language Templates: User Template One

Home Menu Reporting **Notification** Sponsor Settings Guest Accounts Device Accounts Event Codes Common Getting Started Timezones Phone Codes

The following variables should be used to customise the e-mail message:

- %USERNAME%
- %PASSWORD%
- %PAYMENTAMOUNT%
- %STARTTIME%
- %ENDTIME%
- %TIMEZONE%
- %FIRSTNAME%
- %LASTNAME%
- %MOBILENUMBER%
- %MOBILENUMBER_ONLY%
- %COUNTRYCODE%
- %TIMEPROFILE%
- %OPTION1%
- %OPTION2%
- %OPTION3%
- %OPTION4%
- %OPTION5%
- %DATAUSAGE_UP%
- %DATAUSAGE_DOWN%
- %DATAUSAGE_TOTAL%

Select Template for: Guest Print Template (Start End/From Creation) Show

Email Subject: Guest User Account Details

You don't have permission to send Email messages: You don't have permission to send Email messages

Email Text Only Body: The following guest user account has been created for you
Username: %USERNAME%

4. In the Page Body text field, edit the default HTML code for the web page. The Page Body contains all the HTML code that appears between the BODY tags on a HTML page. All HTML code outside these tags is used by the application.
5. In the HTML code you can use the following special variables to replace them with the details from the created User account.
 - %USERNAME% = The Username created for the User.
 - %PASSWORD% = The Password created for the User.
 - %STARTTIME% = The time from which the User account will be valid.
 - %ENDTIME% = The time at which the User account will expire.
 - %FIRSTNAME% = The first name of the User.
 - %LASTNAME% = The last name of the User.
 - %TIMEZONE% = The timezone of the user.

- %MOBILENUMBER% = The mobile number of the User.
- %OPTION1% = Optional field 1.
- %OPTION2% = Optional field 2.
- %OPTION3% = Optional field 3.
- %OPTION4% = Optional field 4.
- %OPTION5% = Optional field 5.
- %MOBILENUMBER_ONLY% = Mobile phone number of User without country code pre- pended.
- %COUNTRYCODE% = Country code of the mobile phone number.
- %DURATION% = Duration of time for which the account will be valid.
- %ALLOWEDWINDOW% = The time window during which the account can be used after first login.
- %TIMEPROFILE% = The name of the time profile assigned.

6. Click the Save button to save your changes.

Editing the Guest Email Template

The Guest Email Template page contains the User account details that the sponsor can email to the User after creating the account.

TIP - Navigating to Account Management > Manage Accounts on the sponsor interface and clicking the Email button next to the User account entry brings up the output of the Email Template and also emails the User.

1. Go to Sponsor Portal > Language Templates and click the underlined name of the template you wish to edit in the Templates list.
2. Under Edit Home Page, click the Notification tab to bring up the Edit Notification Page as shown below.
3. From the Select Template for dropdown menu, choose Guest Email Template and click the Show button.

Language Templates: User Template One

Home Menu Reporting **Notification** Sponsor Settings Guest Accounts Device Accounts Event Codes Common Getting Started Timezones Phone Codes

The following variables should be used to customise the e-mail message:

- %USERNAME%
- %PASSWORD%
- %PAYMENTAMOUNT%
- %DURATION%
- %FIRSTNAME%
- %LASTNAME%
- %MOBILENUMBER%
- %MOBILENUMBER_ONLY%
- %COUNTRYCODE%
- %TIMEPROFILE%
- %OPTION1%
- %OPTION2%
- %OPTION3%
- %OPTION4%
- %OPTION5%
- %DATAUSAGE_UP%
- %DATAUSAGE_DOWN%
- %DATAUSAGE_TOTAL%

Select Template for:

Email Subject:

You don't have permission to send Email messages:

Email Text Only Body:

4. Change the Email Subject as desired.
5. In the Email Body text field, edit the default email text to be sent to the guest page.
6. In the Email Body you can use the following special variables to replace them with the details from the created User account.
 - %USERNAME% = The Username created for the User.
 - %PASSWORD% = The Password created for the User.
 - %STARTTIME% = The time from which the User account will be valid.
 - %ENDTIME% = The time at which the User account will expire.
 - %FIRSTNAME% = The first name of the User.
 - %LASTNAME% = The last name of the User.
 - %TIMEZONE% = The timezone of the user.
 - %MOBILENUMBER% = The mobile number of the User.
 - %OPTION1% = Optional field 1.
 - %OPTION2% = Optional field 2.
 - %OPTION3% = Optional field 3.
 - %OPTION4% = Optional field 4.
 - %OPTION5% = Optional field 5.
 - %MOBILENUMBER_ONLY% = Mobile phone number of User without country code pre- pended.

- %COUNTRYCODE% = Country code of the mobile phone number.
- %DURATION% = Duration of time for which the account will be valid.
- %ALLOWEDWINDOW% = The time window during which the account can be used after first login.
- %TIMEPROFILE% = The name of the time profile assigned.

7. Click the Save button to save your changes

Editing the Guest SMS Template

The Guest SMS Template page contains the User account details that the sponsor can text message to the User after creating the account. The contents of the text message can be fully customized.

TIP - Navigating to Account Management > Manage Accounts on the sponsor interface and clicking the SMS button next to the User account entry brings up the output of the SMS Template and also text messages the User.

1. Go to Sponsor Portal > Language Templates and click the underlined name of the template you wish to edit in the Templates list.
2. Under Edit Home Page, click the Notification tab to bring up the Edit Notification Page as shown below.
3. From the Select Template for dropdown menu, choose Guest SMS Template and click the Show button.

Language Templates: User Template One

Home Menu Reporting **Notification** Sponsor Settings Guest Accounts Device Accounts Event Codes Common Getting Started Timezones Phone Codes

The following variables should be used to customise the e-mail message:

- %USERNAME%
- %PASSWORD%
- %PAYMENTAMOUNT%
- %STARTTIME%
- %ENDTIME%
- %TIMEZONE%
- %FIRSTNAME%
- %LASTNAME%
- %MOBILENUMBER%
- %MOBILENUMBER_ONLY%
- %COUNTRYCODE%
- %TIMEPROFILE%
- %OPTION1%
- %OPTION2%
- %OPTION3%
- %OPTION4%
- %OPTION5%
- %DATAUSAGE_UP%
- %DATAUSAGE_DOWN%
- %DATAUSAGE_TOTAL%

Select Template for: Guest SMS Template (Start End/From Creation) Show

SMS Subject:

SMS Destination:

You don't have permission to send SMS messages: You don't have permission to send SMS messages

SMS Body: The following guest user account has been created for you:

4. Change the SMS Subject as desired.
5. Change the SMS Destination to be the email address of the SMS gateway that you use.

To send the text message to the mobile phone number of the User, use the variable % MOBILENUMBER%. The %MOBILENUMBER% variable is replaced by the mobile phone number, including country code of the User as entered by the sponsor. For example, if the country code selected is the UK (+44) and the User's phone number is 055 555-5555, then % MOBILENUMBER% will contain 44555555555.

Note: The initial plus symbol (+) is not inserted and the initial 0, any spaces, or hyphens (-) are removed from the phone number. If you need (+) to be inserted, then enter +% MOBILENUMBER%.

6. The SMS Body contains the SMS text to be sent to the User. In the SMS Body you can use the following special variables to replace them with the details from the created User account.
 - %USERNAME% = The Username created for the User.
 - %PASSWORD% = The Password created for the User.
 - %STARTTIME% = The time from which the User account will be valid.
 - %ENDTIME% = The time at which the User account will expire.
 - %FIRSTNAME% = The first name of the User.
 - %LASTNAME% = The last name of the User.
 - %TIMEZONE% = The timezone of the user.
 - %MOBILENUMBER% = The mobile number of the User.

- %OPTION1% = Optional field 1.
- %OPTION2% = Optional field 2.
- %OPTION3% = Optional field 3.
- %OPTION4% = Optional field 4.
- %OPTION5% = Optional field 5.
- %MOBILENUMBER_ONLY% = Mobile phone number of User without country code pre- pended.
- %COUNTRYCODE% = Country code of the mobile phone number.
- %DURATION% = Duration of time for which the account will be valid.
- %ALLOWEDWINDOW% = The time window during which the account can be used after first login.
- %TIMEPROFILE% = The name of the time profile assigned.

7. Click the Save button to save your changes.

Deleting a Template

1. From the administration interface, select Sponsor Portal > Language Templates from the left hand menu.
2. Select the template you want to delete from the User Interface Templates list and click the dustbin icon to the right of the template name field.
3. Confirm deletion of the template.

Setting the Sponsor Interface Defaults

1. From the administration interface, select Sponsor Portal > Interface Settings to bring up the Sponsor Defaults page as shown below and click on the Sponsor Defaults tab.

Interface Settings

Sponsor Defaults Login Page Message

Default Language Template: English (Default) ▼

Default Theme: Default Meru Connect ▼ 🔍

Default High Contrast Theme: Default Meru Connect High Contrast ▼ 🔍

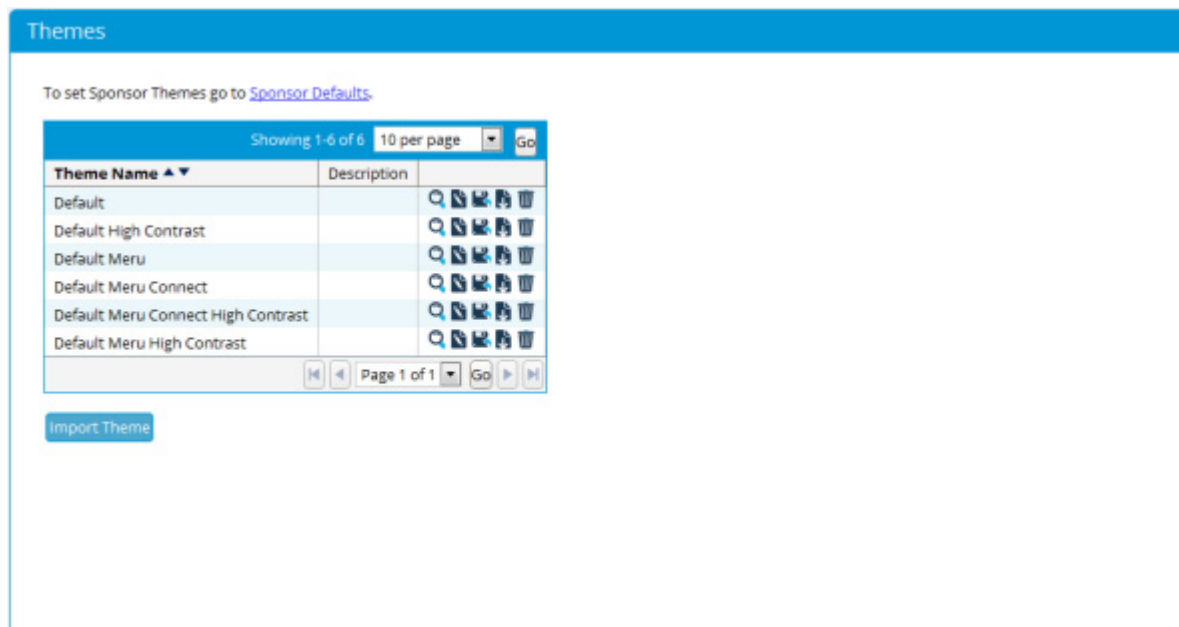
Save

2. Select the Default Language Template from the drop down menu provided. Default will be selected if no Default Language Templates have been created. This is used for the login screen and the template the sponsor uses the first time they login.
3. Select the Theme from the drop down menu provided. Default will be selected if no themes have been created. Click on the preview link to see what your theme will look like before applying.
4. Select the High Contrast Theme from the drop down menu provided. Default will be selected if no High Contrast Themes have been created. Click on the preview link to see what your theme will look like before applying.
5. Click the Save button.

Sponsor Themes

Sponsor Themes can be created specifically for your organizations branding needs and are stored on the FortiConnect.

1. From the administration interface go to Sponsor Portal > Themes as show below.



2. A list of Sponsor Themes are shown:
 - Click on the Disk icon to Copy the selected theme.
 - Click on the Edit icon to Edit the selected theme
 - Click on the Export Icon to Export the selected theme.
 - Click on the Bin icon to Delete the selected theme.
 - Click on the Preview link to Preview the selected theme.
3. To set a Sponsor Theme from the list see the Sponsor Defaults Section.
4. To import a theme that has been created specifically for your requirements, click on the Import Theme button and locate and select your theme.

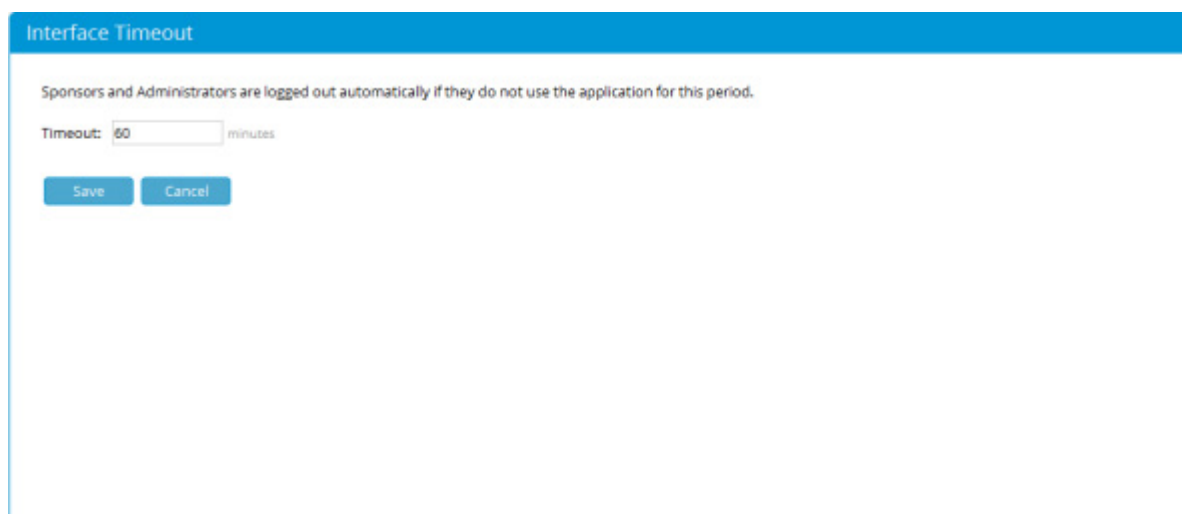
Note: Themes can be created and then imported onto the FortiConnect database to suit your organizations specific requirements.

Session Timeouts

A sponsor or administrator that logs in to the FortiConnect is logged out after a period of inactivity. You can set the inactivity period through the Session Timeout Settings page.

Note: The Session Timeout defined here applies to both the Sponsor and Administration interfaces.

1. From the administration interface, select Server > Interface Timeout from the menu as shown below.



Interface Timeout

Sponsors and Administrators are logged out automatically if they do not use the application for this period.

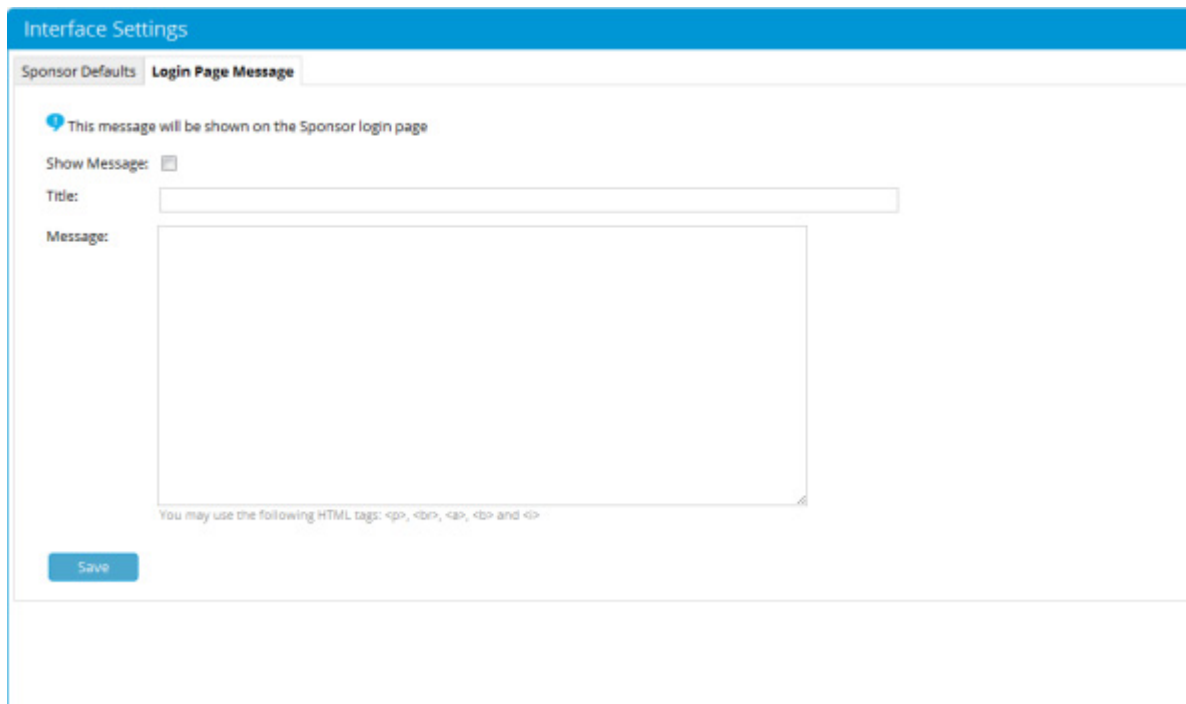
Timeout: minutes

2. Enter the Session Timeout value in minutes (default is 10 minutes). When users are inactive for this amount of time, their sessions expire and the next action they perform takes them to the login page.
3. Click the Save button to save the session timeout.

Login Page Message

Administrators can place a message onto the Sponsors login page if they need to be alerted or notified of anything.

1. From the Admin interface, go Sponsor Portal-->Interface Settings and click on the Login Page Message tab.



The screenshot shows the 'Interface Settings' window with the 'Login Page Message' tab selected. At the top, a blue header bar contains the text 'Interface Settings'. Below the header, there are two tabs: 'Sponsor Defaults' and 'Login Page Message'. The 'Login Page Message' tab is active. Inside the tab, there is a blue information icon followed by the text 'This message will be shown on the Sponsor login page'. Below this, there is a 'Show Message:' label followed by an unchecked checkbox. Underneath the checkbox, there are two input fields: 'Title:' followed by a single-line text box, and 'Message:' followed by a larger multi-line text box. At the bottom of the multi-line text box, there is a small note: 'You may use the following HTML tags: <p>,
, <a>, and <i>'. At the bottom left of the form, there is a blue 'Save' button.

2. To display a message on the Sponsor Interface place a check in the Show Message check box.
3. Enter a Title of your message in the Title field.
4. Enter the content of your message into the Message field.
5. Click Save when completed.

Configuring Portals

Portals on the FortiConnect are used to allow administrators to create their own portal pages and host them on the FortiConnect.

Portals created by administrators can be fully customized and used as the portal to provide the following:

- Customized authentication pages—Allow portal pages to be located on the FortiConnect instead of on each captive portal device, providing a centralized location for configuration and display.
- Guest Self Service—Allows Users to self register by entering their details to create their own User accounts.
- Credit Card Billing support—Enables administrators to allow guests to purchase guest accounts by linking into payment gateways to purchase accounts.
- PMS Integration - Property Management System Integration
- Smart Connect - Secure Smart Connect provisioning for devices.

This chapter explains the following:

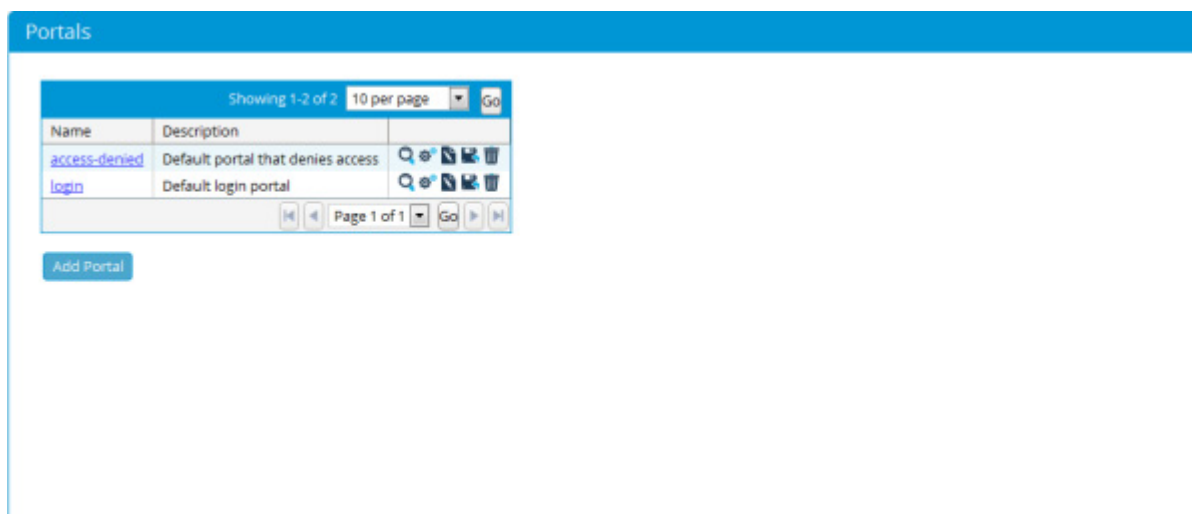
- Configuring Portals Sites
- Configuring Payment Providers
- Creating Portal Web Pages
- Event Codes

Portal Wizard

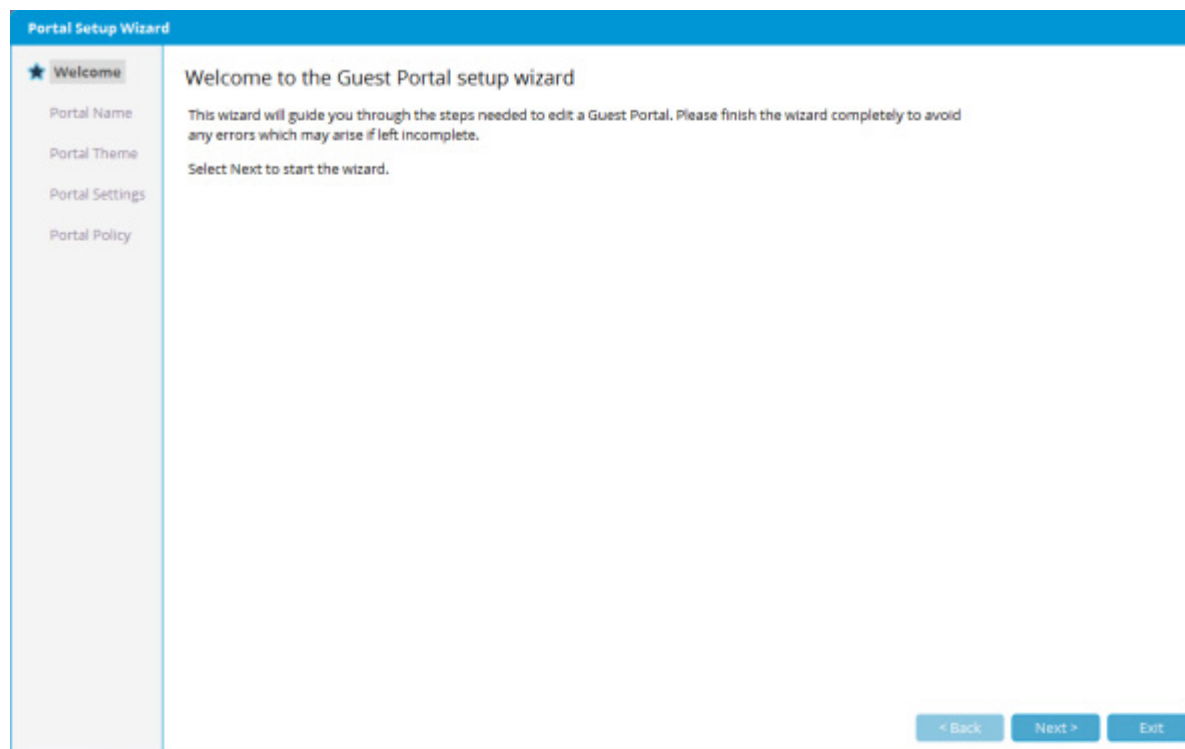
When adding a Portal Site, the FortiConnect will take you through the Portal Wizard to enable easy setup.

1. From the FortiConnect Admin interface, select Guest Portals-->Portals as shown below.

Portal Wizard

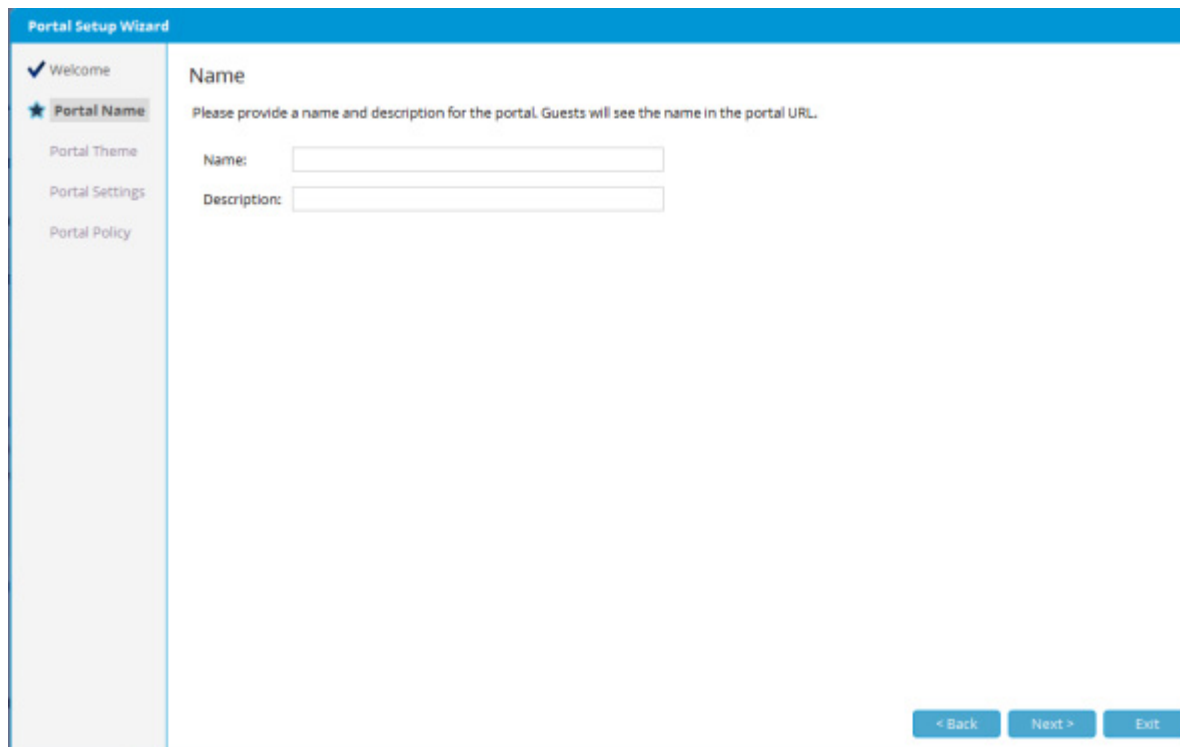


2. Click on the Add Portal button to bring up the Portal Wizard as shown below.



3. Now click on Next to start the wizard and bring up the Basic Settings page.

Creating a Portal

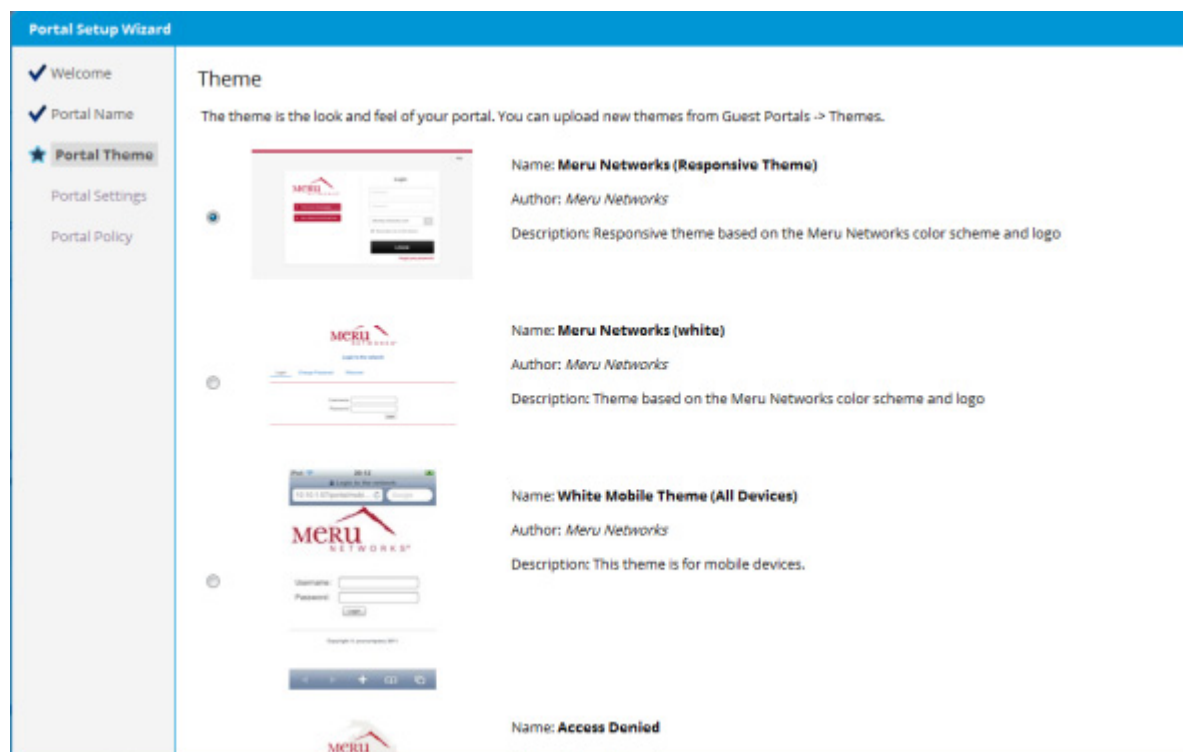


The screenshot shows the 'Portal Setup Wizard' interface. On the left is a sidebar with a list of steps: 'Welcome' (checked), 'Portal Name' (selected with a star icon), 'Portal Theme', 'Portal Settings', and 'Portal Policy'. The main area is titled 'Name' and contains the instruction: 'Please provide a name and description for the portal. Guests will see the name in the portal URL.' Below this are two input fields: 'Name:' and 'Description:'. At the bottom right of the main area are three buttons: '< Back', 'Next >', and 'Exit'.

4. Enter a Site Name and a Site Description, note that the name you enter will be visible by Portal users as it will be part of the site url.
5. Click on Next to continue

Creating a Portal

You will then be required to create the rest of the Portal, the first selection you will have to make is as shown below.:

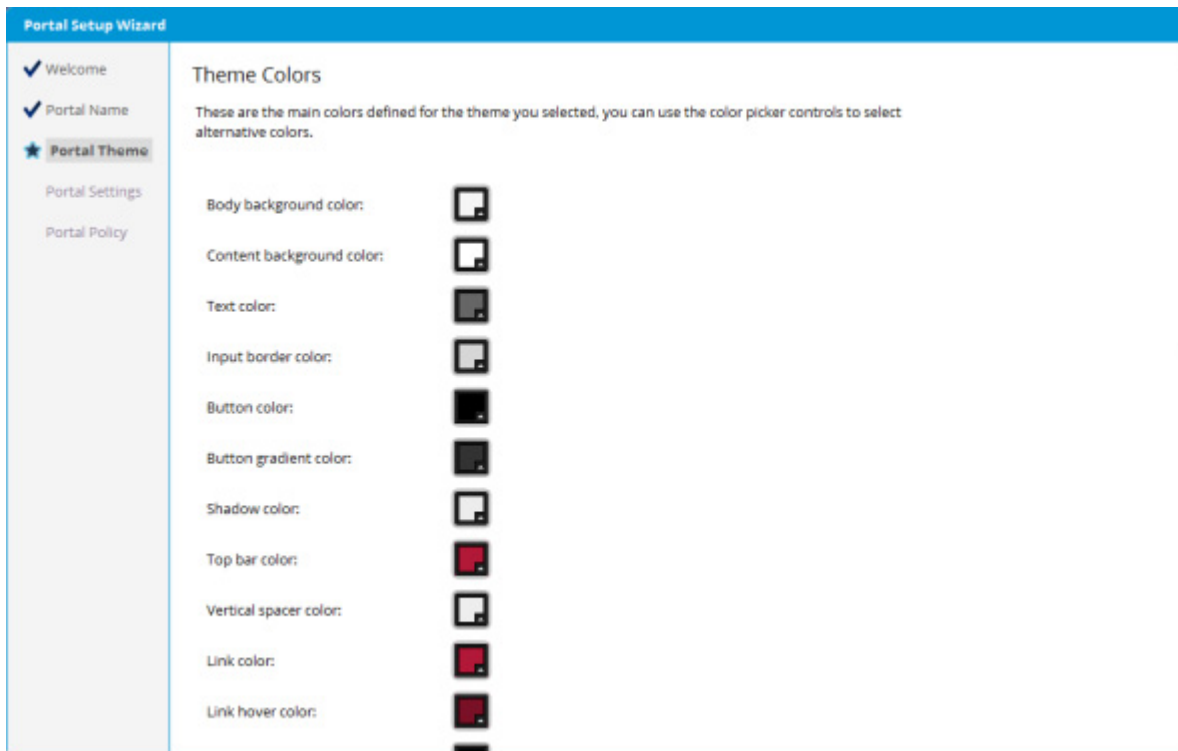


1. Select a predefined Portal Theme as shown above (contact Fortinet to create a customized theme for your company), you can also upload new themes via Guest Portals --> Themes.

Note: You will be asked to confirm your selection and be made aware that changing the theme will result in the new theme definition being used throughout the rest of the portal. Click Yes to acknowledge.

2. Click on Next.

Creating a Portal



3. Select a color scheme for your Portal Theme, click on the relevant boxes next to the text to change their color.
4. Click on Next to continue.

Portal Setup Wizard


- ✓ Welcome
- ✓ Portal Name
- ★ **Portal Theme**
- Portal Settings
- Portal Policy

Theme Images

The images will be used on the Portal.

Supported file formats are JPG, GIF and PNG. Using larger images may result in the portal not looking as the theme intended.


Company logo large:



No file chosen

It is recommended you use an image with 300x40 pixels.


Company logo medium:



No file chosen

It is recommended you use an image with 170x70 pixels.

Company logo small:



No file chosen

It is recommended you use an image with 170x70 pixels.

5. Select a corporate image to use with your Portal.

6. Click Next to continue.

Portal Setup Wizard

✓ Welcome
✓ Portal Name
✓ Portal Theme
★ **Portal Settings**
Portal Policy

Portal Pages

Specify which pages your portal should have enabled and at what stage they should be available.

Page	Displayed in menu	
	Pre-Authentication	Post-Authentication
Login	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Password Change	<input type="checkbox"/>	<input type="checkbox"/>
Self Service	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Device Registration	<input type="checkbox"/>	<input type="checkbox"/>
Credit Card Billing	<input type="checkbox"/>	<input type="checkbox"/>
Successful Authentication	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Welcome Back	<input type="checkbox"/>	<input type="checkbox"/>
Smart Connect	<input type="checkbox"/>	<input type="checkbox"/>
PMS Billing	<input type="checkbox"/>	<input type="checkbox"/>
Access without Login	<input type="checkbox"/>	<input type="checkbox"/>
Password Recovery	<input type="checkbox"/>	<input type="checkbox"/>
My Account	<input type="checkbox"/>	<input type="checkbox"/>
Help	<input type="checkbox"/>	<input type="checkbox"/>
Welcome	<input type="checkbox"/>	<input type="checkbox"/>

Session Management

Allow user to close existing sessions when the concurrent session limit is exceeded: ☒

WiFi Marketing Integration

Enable WiFi Marketing Integration: ☐

Logout Options

Enable Logout Button: ☒
Enable Logout Pop-up window: ☒

7. You can add or remove features to the Portal by modifying the selection of pages that should be available to users as shown above. In each case, select Pre-Authentication to make the feature available before authentication, select Post-Authentication to make the feature available after authentication, or leave both check boxes blank to disable that feature.

Select :

- Login - Display a screen that will allow a user to Login in.
- Password Change - Display a screen allowing the user to change their password.
- Self Service - Display a screen that allows a user to create their own account using Self Service.
- Device Registration - Display a screen that enables a user to register their own device.
- Credit Card Billing- Display a screen that enables Credit Card Billing.
- Successful Authentication - Display a screen that shows Successful Authentication.
- Welcome Back - Display a welcome back page if the user has authenticated previously.
- Smart Connect - Check to enable Smart Connect on the portal.
- PMS Billing - Display a screen that enables PMS Billing.
- Access Without Login - Allow access without having to authenticate.
- Password Recovery - Display a page allowing password recovery options.

- **My Account** - Display 'My Account' details for the user to manage their account once logged in.

My Account page offers following features after log in for the user.

- View account details
- Change password provided when change password feature is enabled
- Detail If it is a purchased account
- List all the payments a User made to purchase access plans
- Printing purchased receipts
- If logged in as an active account
- Top-up a Users usage by extending account time and data allowance by purchasing an Access Plan
- If logged in as expired account
- Reactivate their account to get connect to the network
 - **Help** - Display a Help page screen. (optional page)
 - **Welcome** - Display a Welcome page screen. (optional page)

8. Session Management -

- Allow users to close existing sessions when the concurrent session limit is exceeded - Check to allow users to close existing sessions when the concurrent session limit is exceeded.

9. WiFi Marketing Integration -

- Support for 3rd party Wi-Fi based marketing notification services. Wi-Fi Based marketing notification services enables merchants to push promotions and other related notifications to customers in their close proximity

10. Now enter your Logout Options for the user :-

- **Enable Logout Button** - Check to enable a logout button.
- **Enable Logout Pop-up Window** - Check to enable a pop-up window to logout.

All text on these screens and all Portals can be amended if necessary in Guest Portals --> Portals and by clicking on the Edit icon.

11. Click on Next to continue.

12. Depending on what options you selected in the Portal Pages section above, you will be presented with some or all of the following screens.

Creating a Portal

The screenshot shows the 'Portal Setup Wizard' interface. On the left is a sidebar with a list of steps: 'Welcome', 'Portal Name', 'Portal Theme', 'Portal Settings' (highlighted with a star), and 'Portal Policy'. The main content area is titled 'Remember User on Device'. It contains the following text: 'When configured the user login will be remembered for this device. If the user reconnects to the open network they will be automatically logged in.' followed by 'MAC detection requires that the controller sends the MAC address as part of initial redirection to Meru Connect. This is supported on Meru System Director 6.0 or later, other controllers may not provide this.' and 'If a user obtains access via "Access without Login" page the user will only be remembered if "Remember credentials" is set to "Always".' Below this text are three configuration sections: 'Remember credentials:' with a dropdown menu set to 'Let user choose, default is "off"'; 'Remember for:' with a text input '1' and a dropdown 'Days'; and 'Remember a user by:' with three radio button options: 'Storing encrypted credentials on a cookie in the user's browser', 'Remembering the device they previously logged in with (detected via the MAC address)', and 'Initially attempt to use a cookie, if that fails try the MAC address' (which is selected). At the bottom right are three buttons: '< Back', 'Next >', and 'Exit'.

13. If configured, the users credentials will be remembered for this device. If the user reconnects to the open network they will automatically be logged in using these credentials. MAC detection requires that the controller sends the MAC address as part of initial redirection to IDM. This is supported on Fortinet System Director 6.0 or later, other controllers may not provide this. If a user obtains access via "Access without Login" page the user will only be remembered if "Remember credentials" is set to "Always".
14. Remember Credentials - From the drop down menu select if and how the credentials are stored
15. Remember for - Select how long you wish the credentials to stored for.
16. Remember a user by - How you wish a user to remembered
17. Click on Next once you have selected all your options.

Portal Setup Wizard

- ✓ Welcome
- ✓ Portal Name
- ✓ Portal Theme
- ★ **Portal Settings**
- Portal Policy

Account Options

The following options define what should happen after an account either guest or device is created.

- Auto login — If this option is selected the user will be presented with a login button that will allow them to authenticate without having to type in the new account credentials.
- Display account details - If this option is selected the new account credentials will be displayed on the screen.
- Send account details via SMS - If this options is selected the new account credentials will be sent to the user's mobile phone.
- Send account details via e-mail - If this options is selected the new account credentials will be sent to the user's e-mail address.
- Send purchase receipt by e-mail - If this options is selected a receipt for purchased account will be sent to the user's e-mail address.

Auto Login: ☐

Display account details: ☒

Send account details by SMS: ☒

Send account details by e-mail: ☒

Send purchase receipt by e-mail: ☐

Self Service Account Verification Options

No verification required: ☐

Use event codes: ☒

Use sponsor approval: ☒

Device Registration Verification Options

Use sponsor approval: ☒

Smart Connect Options

Smart Connect language template:

< Back Next > Exit

18. Define what should happen after the account has been created :-

- Auto Login - Select so the user will be presented with a login button that will allow them to authenticate without having to type in the new account credentials.
- Display Account Details - Select to display the new account details on screen.
- Send Account Details by SMS - Select to send the new account details to the users mobile phone.
- Send Account Details by e-mail - Select to send the new account details to the users e-mail address.
- Send Purchase Receipt by e-mail - If this option is selected a receipt for a purchased account will be sent to the users e-mail address.

19. Under the Self Service Account Verification Options, select :-

- Use Event Codes - If enabled the user will be required to provide a valid event code for an account to be generated.
- Use Sponsor Approval - Select so that a sponsor must approve the account before it is activated.

20. Under the Device Registration Verification Options, select :-

- Use Sponsor Approval - Select so that a sponsor must approve the account before it is

activated.

21. Under the Smart Connect Options, select :-

- Smart Connect Language Template - From the drop down menu select the language to be used by the Smart Connect Apps.

22. Click on Next once you have selected all your options.

The screenshot shows the 'Portal Setup Wizard' interface. On the left is a sidebar with navigation links: 'Welcome', 'Portal Name', 'Portal Theme', 'Portal Settings' (highlighted with a star), and 'Portal Policy'. The main content area is titled 'Sponsor Approval Options' and contains a list of options with checkboxes and input fields. The options are: 'Send notification to guest when account is rejected' (checkbox), 'Verify sponsor e-mail' (checkbox), 'E-mail sponsor on approval time out' (checkbox, checked), 'Sponsor e-mail' (text input field), 'Approval times out in' (input field with '0' and a dropdown menu set to 'Hours'), and 'Send notifications until account is dealt with' (checkbox). At the bottom right are three buttons: '< Back', 'Next >', and 'Exit'.

23. Define the Sponsor Approval Options, what should happen when a User account needs approval by a sponsor :-

- Send notification to Guest when account is rejected - When enabled Users will receive an e-mail and/or SMS message letting them know their account requests have been rejected.
- Verify sponsor e-mail - If this option is enabled the e-mail address entered by the User will be validated against the internal sponsor database and authentication servers.
- E-mail sponsor on approval time out - If this is enabled, an e-mail message will be sent to a designated e-mail address after the defined time out period.
- Sponsor e-mail - The e-mail address of the sponsor in charge of dealing with User accounts waiting for approval.
- Approval times out in - The time window sponsors have to approve or reject the account before a notification e-mail is sent to the designated sponsor.

- Send notifications until account is dealt with - If this option is enabled notification e-mails will be sent out recurrently until the account is approved, rejected or expires.

24. Click on Next once this has been complete.

Portal Setup Wizard

- ✓ Welcome
- ✓ Portal Name
- ✓ Portal Theme
- ★ **Portal Settings**
- Portal Policy

Notification Options

This step allows you to set e-mail and SMS header fields.
You should use the following variables to build the SMS destination field so it complies with your SMS gateway requirements

- %MOBILENUMBER% - The mobile number of the guest.
- %MOBILENUMBER_ONLY% - Mobile phone number of guest without country code pre-pended.
- %COUNTRYCODE% - Country code of the mobile phone number.

E-Mail from field:

SMS from field:

SMS to field:

Password Recovery Options

Send Via:

< Back Next > Exit

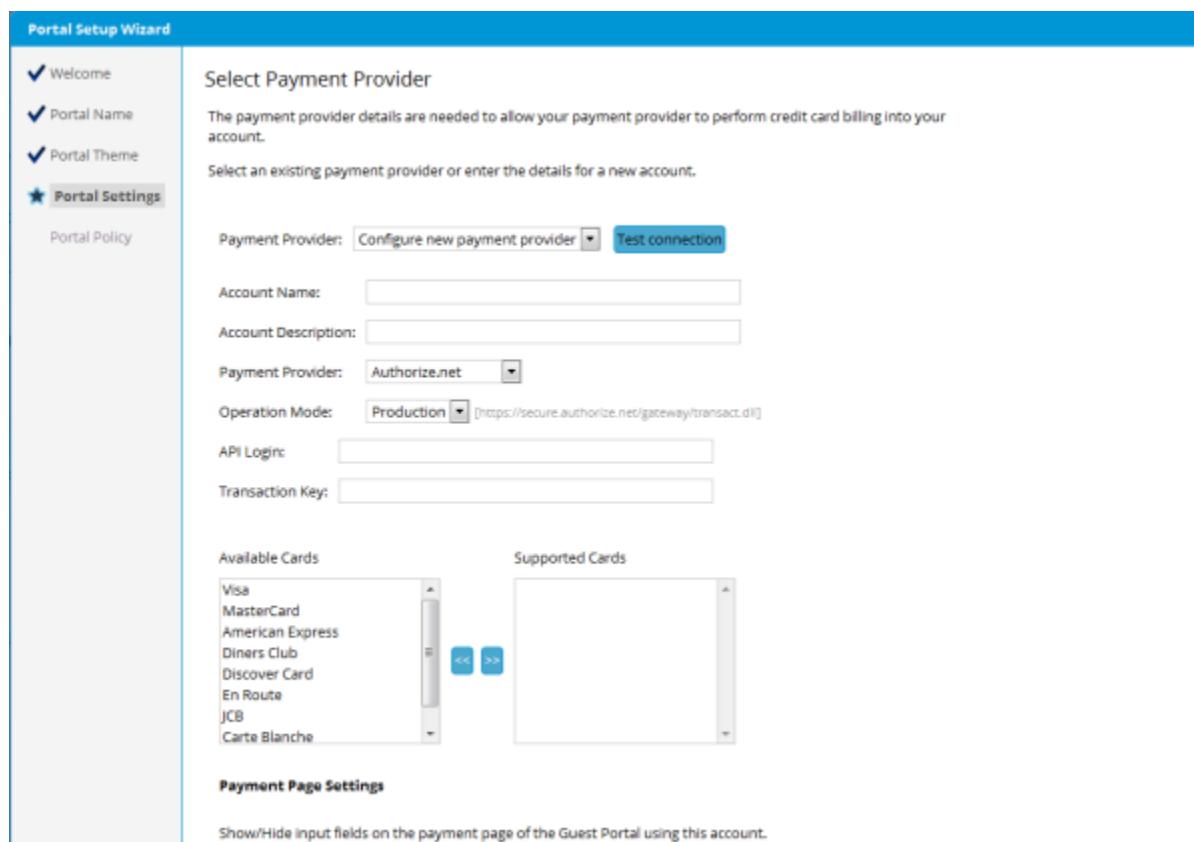
25. Define your Notification Options, this allows you to set up e-mail and SMS header fields.

- E-Mail from field - Enter the E-Mail from address in this field.
- SMS from field - Enter the SMS from address in this field.
- SMS to field - Enter the SMS to address string in this field.

26. Define how FortiConnect will send out a password when Password Recovery has been selected, from the drop down menu, choose from -

- Email Only
- SMS Only
- Both Email and SMS
- Email then if not successful via SMS
- SMS then if not successful via Email

27. Click on Next when you have finished.



28. Select your Payment Provider details, these are needed to allow your payment provider to perform credit card billing into your account :-

- **Payment Provider** - From the drop down menu, Configure a new payment provider, or select a pre-configured payment provider. You can click on the **Test connection** button to test a transaction by sending gateway specific details to the payment provider.
- **Account Name** - Enter a name for your account.
- **Account Description** - Enter a description for your account.
- **Payment Provider** - From the drop down menu, select a payment provider.
- **Operation Mode** - From the drop down menu choose between it being a Production or Test interface.
- **API Login** - Enter the API login details.
- **Transaction Key** - Enter the transaction key details.
- **Available Cards** - Move any supported cards from the Available Cards section to the Supported Cards section using the arrows provided.

29. In the Payment Page Settings section, you can show or hide the input fields on the payment page of the Portal, determine whether you wish use each field using the drop down menu -

- Required - Field requires input
- Optional - Field can be left blank
- Unused - Field will not appear

30. Click on Next once you have finished.

The screenshot shows the 'Portal Setup Wizard' interface. On the left, a sidebar lists the steps: 'Welcome', 'Portal Name', 'Portal Theme', 'Portal Settings' (which is highlighted with a star and a grey background), and 'Portal Policy'. The main area is titled 'Select Default Country for the Credit Card Address' and contains the instruction 'Select the country that is displayed by default for the address of a credit card'. Below this, there is a 'Country:' label followed by a dropdown menu currently showing 'United States'. At the bottom right, there are three buttons: '< Back', 'Next >', and 'Exit'.

31. Select a Default Country that is displayed for the Credit Card Address :-

- Country - From the drop down menu select your country.

32. Click on Next to continue.

Creating a Portal

The screenshot shows the 'Portal Setup Wizard' interface. On the left is a sidebar with a list of steps: 'Welcome', 'Portal Name', 'Portal Theme', 'Portal Settings' (which is highlighted with a star and a blue background), and 'Portal Policy'. The main content area is titled 'Select PMS Provider'. It contains the following text: 'The Property Management System details are needed to enable room billing. Select an existing Property Management System or enter the details for a new account.' Below this text is a form with the following fields: 'Property Management System:' with a dropdown menu currently showing 'Configure new Property Management System'; 'Name:' with a text input field; 'Description:' with a text input field; 'Type:' with a dropdown menu currently showing 'HDBIC'; 'IP Address:' with a text input field; and 'Port:' with a text input field. At the bottom right of the form are three buttons: '< Back', 'Next >', and 'Exit'.

33. Select your PMS Provider details, these are needed to enable room billing.

- Property Management System - From the drop down menu choose an existing Property Management System or Configure new Property Management System.

Note: Existing Property Management Systems can be added at Guest Portals --> Hotel PMS

- Name - Enter a name for the Property Management System.
- Description - Enter a description for the Property Management System.
- Type - From the drop down menu, select the type of Property Management System you will be using.
- IP Address - Enter the IP address of the Property Management System.
- Port - Enter the port number.

34. Click on Next to continue.

The screenshot shows the 'Portal Setup Wizard' interface. On the left is a sidebar with a list of steps: 'Welcome' (checked), 'Portal Name' (checked), 'Portal Theme' (checked), 'Portal Settings' (selected with a star icon), and 'Portal Policy'. The main area is titled 'Select Currency' and contains the instruction: 'Select which currencies this portal should use for billing credit cards and Hotel PMS systems.' Below this, there are two dropdown menus: 'Payment Gateway Currency' set to 'Australian Dollar' and 'PMS Currency' set to 'US Dollar'. At the bottom right, there are three buttons: '< Back', 'Next >', and 'Exit'.

- 35.** Select which currencies the portal should use for billing credit cards and for Hotel PMS systems.
- Payment Gateway Currency - Select the currency for your payment gateway.
 - PMS Currency - Select the currency for your Property Management System.
- 36.** Click on Next to continue.

Creating a Portal

Portal Setup Wizard

- ✓ Welcome
- ✓ Portal Name
- ✓ Portal Theme
- ★ **Portal Settings**
- Portal Policy

Access Plans

Manage the access plans users accessing this portal will be able to select.

Access plans allows you to define when and where the user will be allowed to access the network by selecting a Usage Profile and Account Group. You can also specify the cost of purchasing an account if your portal allows this through Credit Card or PMS billing.

Name	Description	Total Price	Currency	Usage Profile	Account Group	Used for
No access plans defined						

Use Access Plan for: Self Service

Name:

Description:

Usage Profile: Unlimited To define Usage Profiles go to Policy Settings -> Usage Profiles

Account Group: Default Account Group To define Account Groups go to Policy Settings -> Account Groups

Pre-tax Price:

Tax: % Leave blank/zero if no tax applies

Total Price:

37. Manage the access plans users accessing the portal will be able to select :-

- Use Access Plan for - From the drop down menu select whether the access plan is for Self Service users, Credit Card Billing, PMS Billing, Device Registration, Access without Login or the My Account option where users can provision their own account after login.
- Name - Enter the name of your plan.
- Description - Enter a description for your plan.
- Usage Profile - From the drop down menu choose from a pre-defined Usage profile. Usage profiles can be defined in Policy Settings --> Usage Profiles.
- Account Group - From the drop down menu choose from a pre-defined Account Group. Account Groups can be defined in Policy Settings --> Account Groups.
- Pre-tax Price - If your time profile is assigned to a billing plan, then enter the price of your plan, pre-tax.
- Tax - Enter the percentage of tax you wish to charge. Leave blank of no tax applied.
- Total Price - The total price of the plan will appear automatically in this field.

38. Click on Add to add your plan.

39. Click on Next to continue.

Portal Setup Wizard

- ✓ Welcome
- ✓ Portal Name
- ✓ Portal Theme
- ✓ Portal Settings
- ★ Portal Policy

Portal Redirect Policy

- Acceptable Usage Policy — Use this option to specify when should guests be shown the Acceptable usage policy.
- Show Acceptable Usage Policy to the user — Use this option to specify when Acceptable usage policy needs accepting by a user after authentication.
- Initial Page — This is the portal page guests will be taken to once they first get on the network.
- After Authentication Redirect To — Use this option to specify where the user should be taken to after a successful authentication.
- First login portal success page — Use this option to specify which portal page first time users should be taken to after authentication.
- Subsequent login portal success page — Use this option to specify which portal page returning users should be taken to after authentication.

Acceptable Usage Policy:

Show Acceptable Usage Policy to the user:

Initial Page:

After Authentication Redirect To:

Redirect to:

It's possible to use the following variables to build the redirect URL.

- %ID% - The account id number.
- %USERNAME% - The account username.
- %FIRSTNAME% - The user's first name.
- %LASTNAME% - The user's last name.
- %MACADDRESS% - The MAC address of the device from which the user is authenticating.

40. You are now presented with the Portal Redirect Policy screen, choose from the following :

- Acceptable Usage Policy - From the drop down menu select whether an acceptable usage policy should be displayed Pre-Authentication, Post-Authentication, or whether it should be Disabled.
- Show Acceptable Usage Policy - From the drop down menu select how often you wish to show the Acceptable Usage Policy, whether it be Every Login, On First Login, and on First Login and any Subsequent Acceptable Usage Policy Changes.
- Initial Page - From the drop down menu select which portal page the Users will be taken to once they first get on the network. Your options will differ depending on the choices you made on the Portal Pages screen previous.
- After Authentication Redirect To - From the drop down menu select as to where the Users should be directed to after a successful authentication.
 - Portal Success Page - Redirect to a Portal Success Page, from the drop down menu select which page you wish to use as a Portal Success Page.
 - Predefined URL - Redirect users to a predefined URL once they authenticate successfully. You can pass certain properties of the User as GET requests of the redirect. To do this, construct the URL using the following placeholders:
 - %ID% - placeholder for the MCT internal id of the authenticated account
 - %USERNAME% - placeholder for the username of the authenticated account
 - %FIRSTNAME% - placeholder for the first name of the authenticated account
 - %LASTNAME% - placeholder for the last name for the authenticated account

- %MACADDRESS% - placeholder for the MAC address of the device of the authenticated account

For example if the customer website is at <http://example.com> and you need info the username of the authenticated user, you configure redirect URL like <http://mywebsite.com?username=%USERNAME%> it would then be up to the customer website to parse and use that information as required.

41. If on the Portal Pages setup screen you chose to display a Welcome Back page after authentication you will see a set of different options to define landing pages as shown below.
42. The option to land at a subsequent portal page if the user is recognized can now be defined -
 - First login portal success page - From the drop down menu select what portal success page a user should land on after first login.
 - Subsequent login portal success page - From the drop down menu select which portal success page a user should land on upon their return.
43. Click on Next to continue.

The screenshot shows the 'Portal Setup Wizard' interface. On the left is a sidebar with a list of steps: Welcome, Portal Name, Portal Theme, Portal Settings, and Portal Policy (which is highlighted with a star). The main content area is titled 'Portal External Authentication Policy'. It contains a sub-header 'Portal External Authentication Policy' and a descriptive text: 'Select which realms should be used for authentication on the login page. If the selection mode is set to automatic internet services such as Google, Facebook and Twitter will always be checked last.' Below this text are two lists: 'Available Realms' containing 'test' and 'Selected Realms' containing 'default'. Between these lists are '<<' and '>>' buttons. To the right of the 'Selected Realms' list are 'Up' and 'Down' buttons. Below the lists is a 'Selection Mode' section with two radio buttons: 'Manual: guests have to select the appropriate realm from "Selected Realms" list.' (which is selected) and 'Automatic: each realm is tried in the order from "Selected Realms" list.' At the bottom right of the screen are three buttons: '< Back', 'Next >', and 'Exit'.

44. Now you can select which realms should be displayed to the User on the login page, the realms are defined on the external Users page Policy Settings --> Account Groups and are used to authenticate Users against different external servers for a realm.

- 45. Portal External Authentication Policy** - If you use OAuth using any of the social login (Facebook, Twitter, and Google), you can specify what social profile information you wish to capture on the MCT database when a user authenticates. This is done through the Guest Portal wizard, new portal stages are displayed when Facebook or Google authentication is enabled for the portal, Twitter does not allow extra user information to be gathered and as such this feature does not apply to it.

On the wizard stage for the different services its possible to select different categories of information, these depend on the service used, you will notice there are more options for Facebook when compared to Google.

When available the user information will be recorded on the MCT database, it will not be visible through any Sponsor/Admin portal reports. The only way to access this information is through the MCT Sponsor API, Any API call that returns account objects will include a <socialProfile> XML element containing the available information for that account.

Note: Only the information authorized by the social app can be collected. In some cases, depending on the type of information this will require the OAuth app to be approved by the OAuth provider, this is outside the scope of the MCT documentation. Also the user has ultimate control over what he/she shares with MCT, if the user refuses to share information MCT will not get access to it.

To enable OAuth in FortiConnect with Fortigate, ensure that you whitelist the following OAuth service provider URLs in the Fortigate Server:

Facebook

```
config firewall address
edit "FB0"
set subnet 5.178.32.0 255.255.240.0
next
edit "FB1"
```

Creating a Portal

```
set subnet 195.27.154.0 255.255.255.0
next
edit "FB2"
set subnet 80.150.154.0 255.255.255.0
next
edit "FB3"
set subnet 77.67.96.0 255.255.252.0
next
edit "FB4"
set subnet 212.119.27.0 255.255.255.128
next
edit "FB5"
set subnet 2.16.0.0 255.248.0.0
next
edit "FB6"
set subnet 66.171.231.0 255.255.255.0
next
edit "FB7"
set subnet 31.13.24.0 255.255.248.0
next
edit "FB8"
set subnet 31.13.64.0 255.255.192.0
next
edit "FB9"
set subnet 23.67.246.0 255.255.255.0
next
edit "akamai-subnet-23.74.8"
set subnet 23.74.8.0 255.255.255.0
next
edit "akamai-subnet-23.74.9"
set subnet 23.74.9.0 255.255.255.0
```



```
next
edit
"akamaihd.net"
set type fqdn
set fqdn "akamaihd.net"
next
edit "channel-proxy-06-frc1.facebook.com"
set type fqdn
set fqdn "channel-proxy-06-frc1.facebook.com"
next
edit "code.jquery.com"
set type fqdn
set fqdn "code.jquery.com"
next
edit "connect.facebook.com"
set type fqdn
set fqdn "connect.facebook.com"
next
edit "fbcdn-photos-c-a.akamaihd.net"
set type fqdn
set fqdn "fbcdn-photos-c-a.akamaihd.net"
next
edit "fbcdn-profile-a.akamaihd.net"
set type fqdn
set fqdn "fbcdn-profile-a.akamaihd.net"
next
edit "fbexternal-a.akamaihd.net"
set type fqdn
set fqdn "fbexternal-a.akamaihd.net"
next
edit "fbstatic-a.akamaihd.net"
```

Creating a Portal

```
set type fqdn
set fqdn "fbstatic-a.akamaihd.net"
next
edit "m.facebook.com"
set type fqdn
set fqdn "m.facebook.com"
next
edit "ogp.me"
set type fqdn
set fqdn "ogp.me"
next
edit "s-static.ak.facebook.com"
set type fqdn
set fqdn "s-static.ak.facebook.com"
next
edit "static.ak.facebook.com"
set type fqdn
set fqdn "static.ak.facebook.com"
next
edit "static.ak.fbcdn.com"
set type fqdn
set fqdn "static.ak.fbcdn.com"
next
edit "web_ext_addr_SocialWiFi"
set type fqdn
set fqdn "web_ext_addr_SocialWiFi"
next
edit "www.facebook.com"
set type fqdn
set fqdn "www.facebook.com"
next
```

```
end
```

Google+

```
config firewall address
```

```
edit "www.googleapis.com"
```

```
set type fqdn
```

```
set fqdn "www.googleapis.com"
```

```
next
```

```
edit "accounts.google.com"
```

```
set type fqdn
```

```
set fqdn "accounts.google.com"
```

```
next
```

```
edit "ssl.gstatic.com"
```

```
set type fqdn
```

```
set fqdn "ssl.gstatic.com"
```

```
next
```

```
edit "fonts.gstatic.com"
```

```
set type fqdn
```

```
set fqdn "fonts.gstatic.com"
```

```
next
```

```
edit "www.gstatic.com"
```

```
set type fqdn
```

```
set fqdn "www.gstatic.com"
```

```
next
```

```
edit "Google_13"
```

```
set subnet 216.58.192.0 255.255.224.0
```

Accounts.google.com is too dynamic for an FQDN policy to function.

This IP policy covers the whole range of possible subnets.

```
next
```

```
end
```

Twitter

```
config firewall address
edit "api.twitter.com"
set type fqdn
set fqdn "api.twitter.com"
next
edit "abs.twimg.com"
set type fqdn
set fqdn "abs.twimg.com"
next
edit "abs-0.twimg.com"
set type fqdn
set fqdn "abs-0.twimg.com"
next
end
```

46. Manual Selection - Select this mode for the user to select an appropriate realm from the 'selected realms' list.

47. Automatic Selection - Select this mode so that each realm is selected in order from the list rather than asking the user to select one. The realm selection starts from the top of the order first and if authentication fails the next realm in the order is tried and so on.

48. The first realm in the order is treated as a default realm, the default realm is selected by default when the user navigates to the Login Page in the Manual Selection mode above.

Note: If Automatic Selection is selected then internet services such as Google, Facebook and Twitter will always be checked last.

49. Click on Next to continue.

50. In the Portal Restrictions page, you can set the time interval that Prevents the creation of self-service accounts with the same personal details (email/phone) for a specified period of time post the original account creation.

Portal Setup Wizard

✓ Welcome

✓ Portal Name

✓ Portal Theme

✓ Portal Settings

★ Portal Policy

Portal Restrictions

Please configure the account re-creation restrictions.

If unrestricted users will be able to create new accounts as expires.

Restriction Length: Days ▼
Set to 0 for unrestricted account creation.

Restriction Type: Email ▼

51. Click on Next to continue.

Creating a Portal

The screenshot shows the 'Portal Setup Wizard' interface. On the left is a sidebar with a list of steps: 'Welcome', 'Portal Name', 'Portal Theme', 'Portal Settings', and 'Portal Policy' (which is highlighted with a star). The main area is titled 'Portal Account Groups Authentication Policy'. It contains the following elements:

- A heading: 'Portal Account Groups Authentication Policy'.
- A paragraph: 'By default guests in all account groups are permitted to authenticate against this portal.'
- A label: 'Account groups permitted to use this portal:' followed by a dropdown menu currently set to 'Selected'.
- Two list boxes: 'Excluded Account Groups' (empty) and 'Permitted Account Groups' (containing 'Default Account Group').
- Two blue arrow buttons (left-pointing and right-pointing) between the list boxes.
- At the bottom right, three buttons: '< Back', 'Next >', and 'Exit'.

52. We can now control which account groups can authenticate against a particular portal (User/device accounts belong to account groups). This is done on the Portal Account Groups Authentication Policy screen. The default behaviour is to permit All account groups.
53. From the drop down menu you choose between All or Selected.
54. If you have chosen to select account groups, use the arrows to place the selected account groups into the Permitted Account Groups section.

Portal Setup Wizard

- ✓ Welcome
- ✓ Portal Name
- ✓ Portal Theme
- ✓ Portal Settings
- ★ **Portal Policy**

Guest Username Policy

The following options allow you to specify how the usernames for the guest accounts created through this portal should be generated.

- Email address as username — The guest e-mail address will be used as the username for the account.
- Create username based on first and last names — The guest's first and last names will be combined to generate the account username.
- Create random username — The username for the account will be randomly generated.
- Username Prefix — This will be used as prefix to generate the account username.

Username Prefix:
All generated usernames will be prefixed with this text.

Email address as username

☒ Email address as username

Create Username With Case:

Enforce unique email: ☐

Create username based on first and last names

☐ Create username based on first and last names

Minimum username length:

Create Username With Case:

Create Username With Separator:

Create random username

☐ Create random username

Alphabetic characters to include:

Number to include:

55. Now you can select and choose your site policy, choose how usernames for User accounts for the Portal should be generated.

- Email address as username - The User e-mail address will be used as the username for the account.
- Create usernames based on first and last name - The Users first name and last names will be combined to generate the account username.
- Create random username - The username for the account will be randomly created.
- Username Prefix - This will be used as a prefix to generate the account username.

56. Click on Next to continue

Creating a Portal

The screenshot shows the 'Portal Setup Wizard' interface. On the left is a sidebar with a list of steps: 'Welcome', 'Portal Name', 'Portal Theme', 'Portal Settings', and 'Portal Policy' (which is highlighted with a star). The main area is titled 'Guest Password Policy' and contains the following sections:

- Guest Password Policy**
By modifying the following options you can define which characters will be used when generating account passwords and how long the password should be.
- Password generation mode**
Two radio buttons are present: 'Auto generated password' (selected) and 'Guest specified password'.
- Password requirements**
This section includes four groups of settings:
 - Alphabetic Characters:** 'Characters to include' is a text box containing 'abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ' with a dropdown showing the same string.
 - Password case:** A dropdown menu set to 'Mixed'.
 - Numeric Characters:** 'Number to include' is a dropdown set to '6'.
 - Numeric Characters:** 'Characters to include' is a text box containing '0123456789' with a dropdown showing the same string.
 - Other Characters:** 'Number to include' is a dropdown set to '2'.
 - Other Characters:** 'Characters to include' is a text box containing a regex string '[!@#\$%^&*()_+=-{}|:~`~<>?]' with a dropdown showing the same string.
 - Other Characters:** 'Number to include' is a dropdown set to '0'.

At the bottom right of the main area are three buttons: '< Back', 'Next >', and 'Exit'.

57. Choose whether you want the passwords to be -

- Auto generated password - password is generated using conditions below
- Guest specified password - password is specified by the user creating the account

58. Choose how passwords for User accounts for the User Portal should be generated.

- Alphabetic Characters - Decide the number of characters to use.
- Numeric Characters - Decide the number of characters to use.
- Other Characters - Decide the number of characters to use.

59. Click on Next to continue.

Portal Setup Wizard

- ✓ Welcome
- ✓ Portal Name
- ✓ Portal Theme
- ✓ Portal Settings
- ★ **Portal Policy**

Guest Account Details

Standard Fields

First Name: Required

Last Name: Required

Company: Unused

Email: Required
This cannot be changed as email address is being used as the username in Username Policy

Mobile: Unused

Additional Fields

Option 1: Unused

Option 2: Unused

Option 3: Unused

Option 4: Unused

Option 5: Unused

< Back Next > Exit

60. Select which fields should be used to capture User Account Details :-

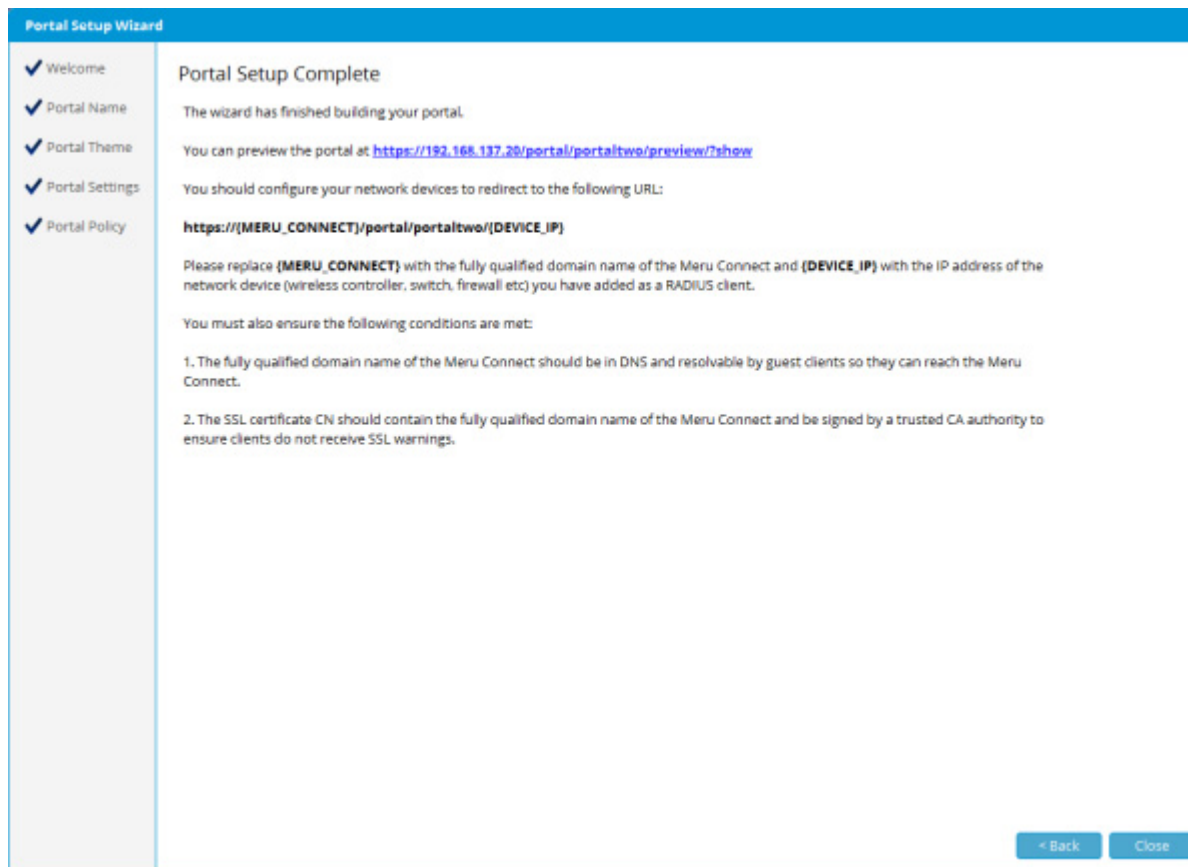
- First Name - From the drop down menu decide whether this field is Required, Unused or Optional.
- Last Name - From the drop down menu decide whether this field is Required, Unused or Optional.
- Company - From the drop down menu decide whether this field is Required, Unused or Optional.
- Email - From the drop down menu decide whether this field is Required, Unused or Optional.
- Mobile - From the drop down menu decide whether this field is Required, Unused or Optional.
- Additional Fields - From the drop down menu decide whether this field is Required, Unused or Optional.

61. Click on Next to continue.

Creating a Portal

The screenshot shows the 'Portal Setup Wizard' interface. On the left is a sidebar with a list of steps: 'Welcome', 'Portal Name', 'Portal Theme', 'Portal Settings', and 'Portal Policy'. The 'Portal Policy' step is currently selected and highlighted with a star icon. The main content area is titled 'Purchase Guest Account Details' and contains the text 'Additional fields can be added to your Purchase Account page.' Below this text are five options, each with a label and a dropdown menu: 'Option 1: Unused', 'Option 2: Unused', 'Option 3: Unused', 'Option 4: Unused', and 'Option 5: Unused'. At the bottom right of the wizard, there are three buttons: '< Back', 'Next >', and 'Exit'.

- 62.** Select how many fields should be used to capture additional information for Purchased Accounts:-
- Option 1 - From the drop down menu decide whether this field is Required, Unused or Optional.
 - Option 2- From the drop down menu decide whether this field is Required, Unused or Optional.
 - Option 3 - From the drop down menu decide whether this field is Required, Unused or Optional.
 - Option 4 - From the drop down menu decide whether this field is Required, Unused or Optional.
 - Option 5 - From the drop down menu decide whether this field is Required, Unused or Optional.
- 63.** Click on Next to continue.



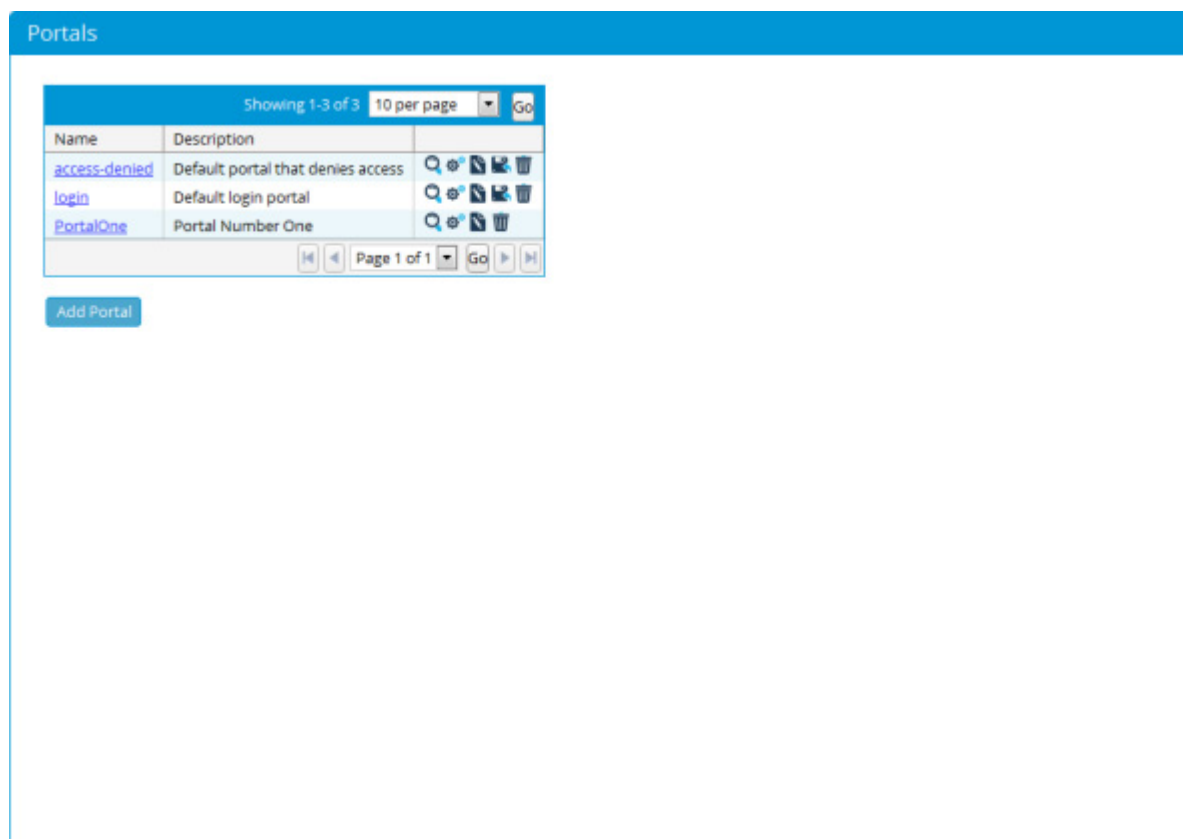
The Portal setup is now complete. Click on Close to finish.

Preview an Existing Portal

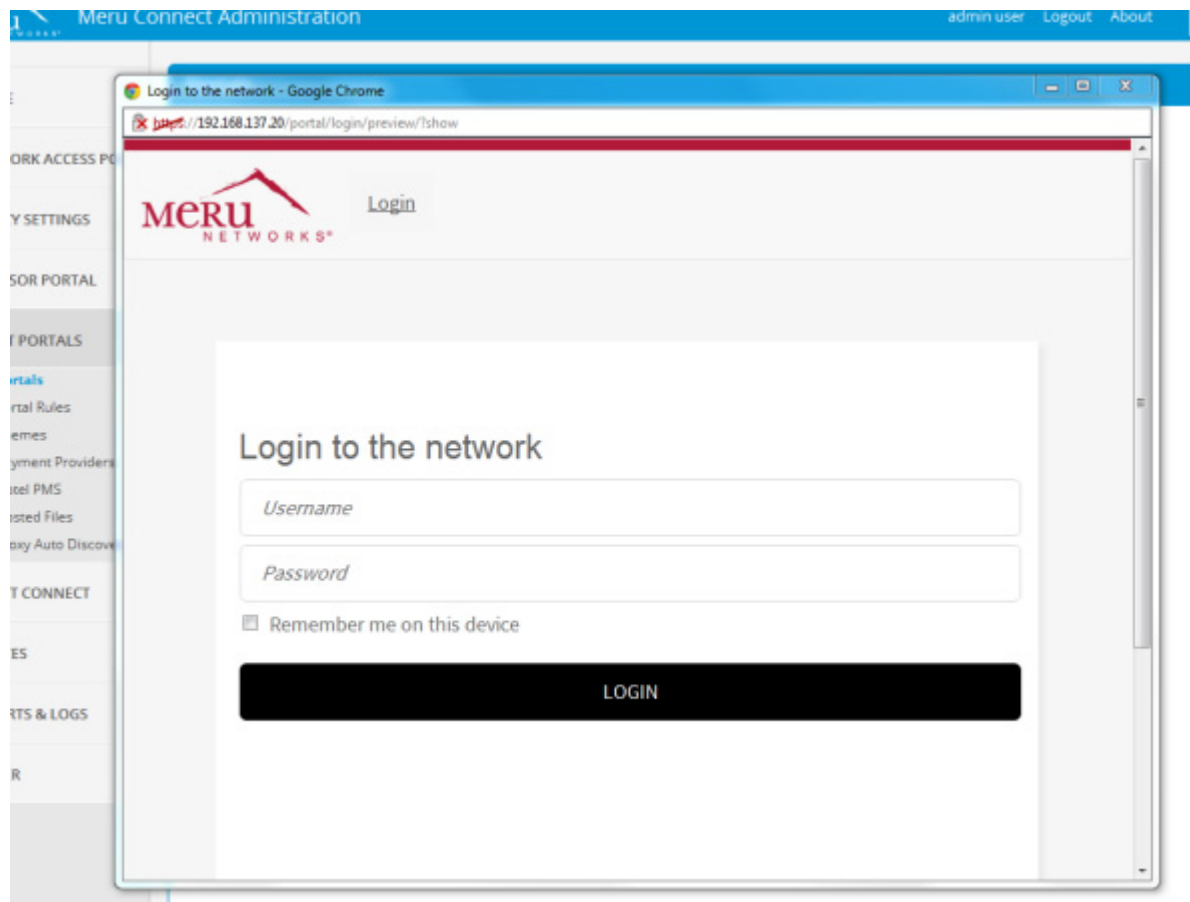
You can preview a Portal once its been setup.

1. From the Administration interface go to Guest Portals --> Portals as shown below.

Preview an Existing Portal

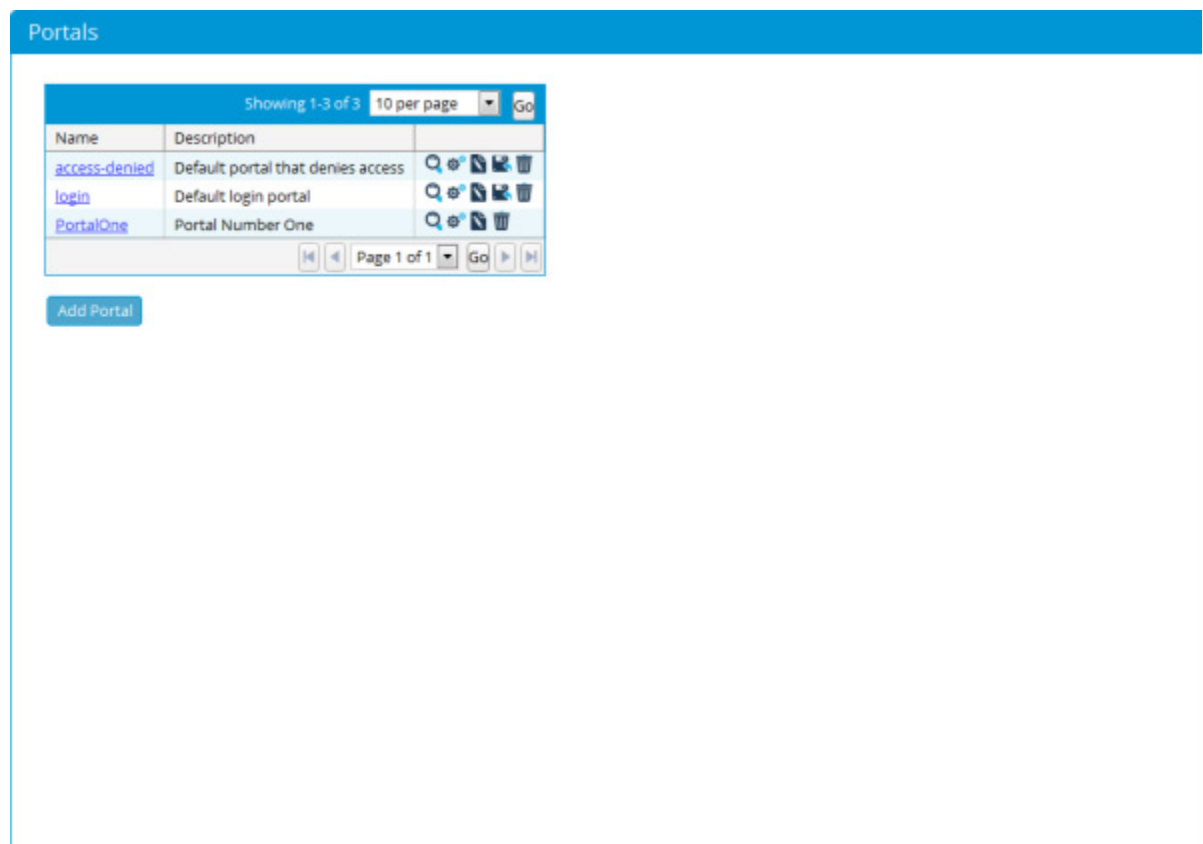


2. Select the Portal you wish to preview by clicking on the Preview Icon next to the Description field.
3. The Portal you have created should then appear as shown below.



Editing Portal Content

Once a Portal has been created, you can edit and customize the content of the Portal, go to Guest Portals --> Portals



1. Choose the portal you wish to edit of its content and click on the edit content icon.

Widget Labels	
Login Page	Please change the text shown on forms and components in the portal.
Acceptable Usage Policy Page	
Logout Page	
Logged Out Page	
iOS auto login Page	
Cookies instructions Page	
Close this window Page	
Authenticating waiting Page	
Session management Page	
Widget Labels	
Status Messages	
Realm Labels	
Windows Smart Connect	
iOS Smart Connect	
iOS Auto Login Smart Connect	
Mac Smart Connect	
Android Smart Connect	
Linux Smart Connect	
Generic Smart Connect	
Approval Notification Email	
Account Rejection Email	
Account Rejection SMS	
"From Creation" Email	
From Creation SMS	

Default Phone Code:	+1
Username:	Username
Password:	Password
Confirm Password:	Confirm Password
Remember me on this device:	Remember me on this device
Realm:	Realm
Login button:	Login
Access without Login button:	Connect
Days:	Days(s)
Hours:	Hour(s)
Minutes:	Minute(s)
Time left text:	Your account will expire in:
Time left calculating:	Calculating...
Time left Unlimited account text:	Your account is unlimited
Try again:	Try again
New password:	New Password
Old Password:	

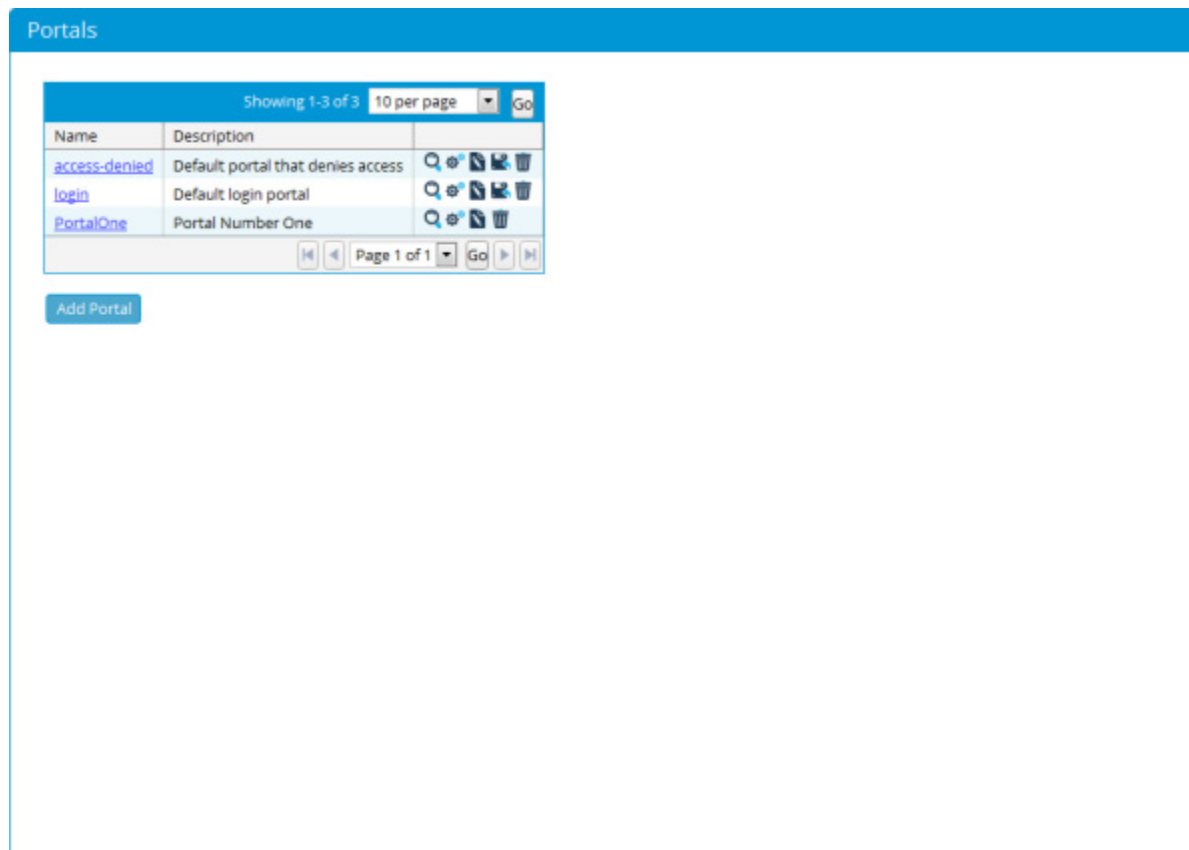
- On the left hand side of the screen you can see all the different pages/options that have been created when the portal was set up using the Portal Wizard. Click on the page/option tab that you wish to edit, for the example above we have selected the LoginPage. You can amend any text within the box and insert your own.
- Click Save once you have amended/added any text.
- Continue to edit another page/option by clicking on the relevant tab.

Edit or Delete an Existing Portal Site

Edit an Existing Portal

You can edit an existing Portal Site from the administration interface.

1. From the administration interface, select Guest Portals --> Portals as shown below.

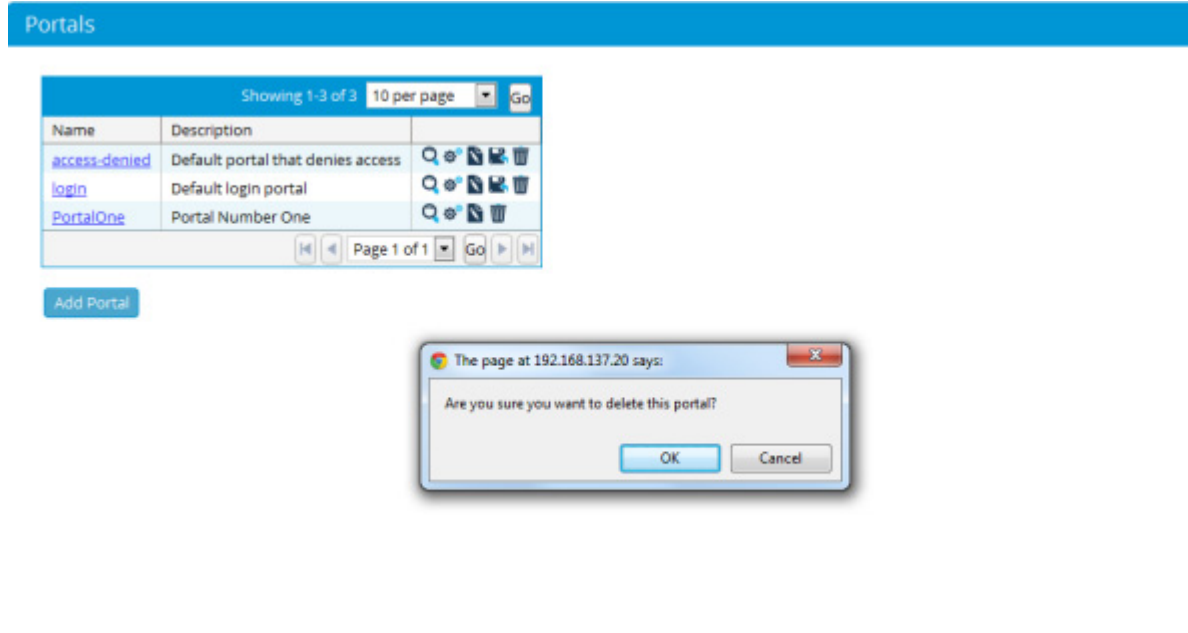


2. Select the portal you want to edit from the list and click the Change Portal Settings icon next to the Description field.
3. You will then be taken through the Portal Wizard setup again, you can make any changes you require via this.

Delete an Existing Portal

You can delete an existing Portal Site from the administration interface.

1. From the administration interface, select Guest Portals --> Portals as shown below.



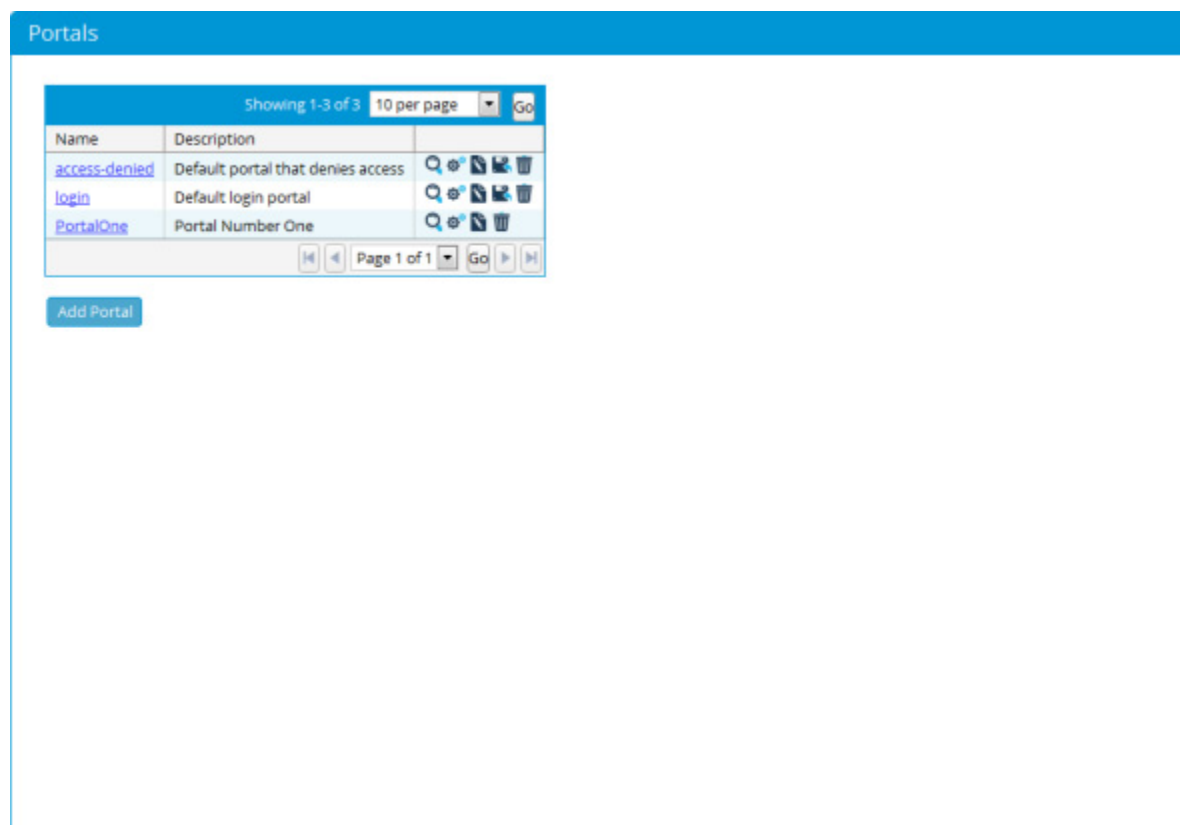
2. Select the portal you wish to delete and click on the Bin icon next the descriptions field.
3. Click Yes to confirm deletion.

Copying a Portal

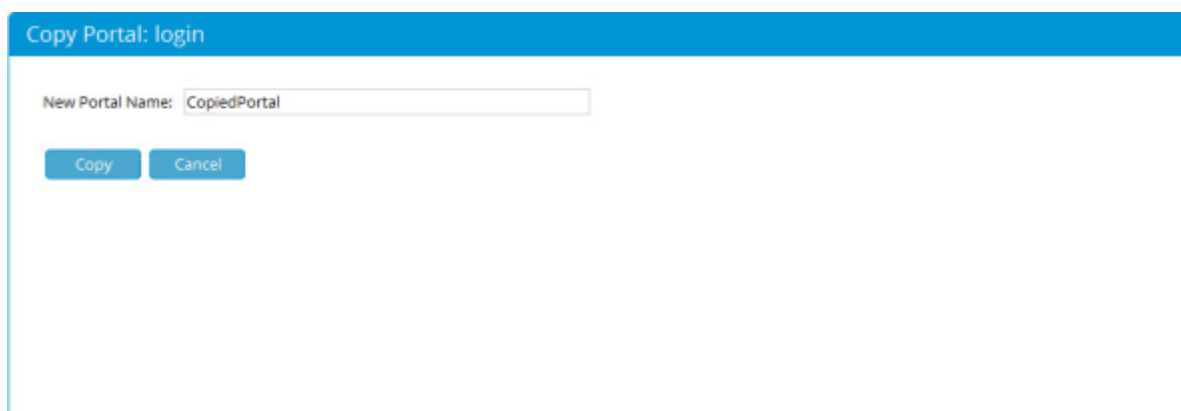
Administrators can copy Portals that have already been created to save time going through the setup wizard if a duplicate portal is needed.

From the Administration interface go to Guest Portals --> Portals as shown below.

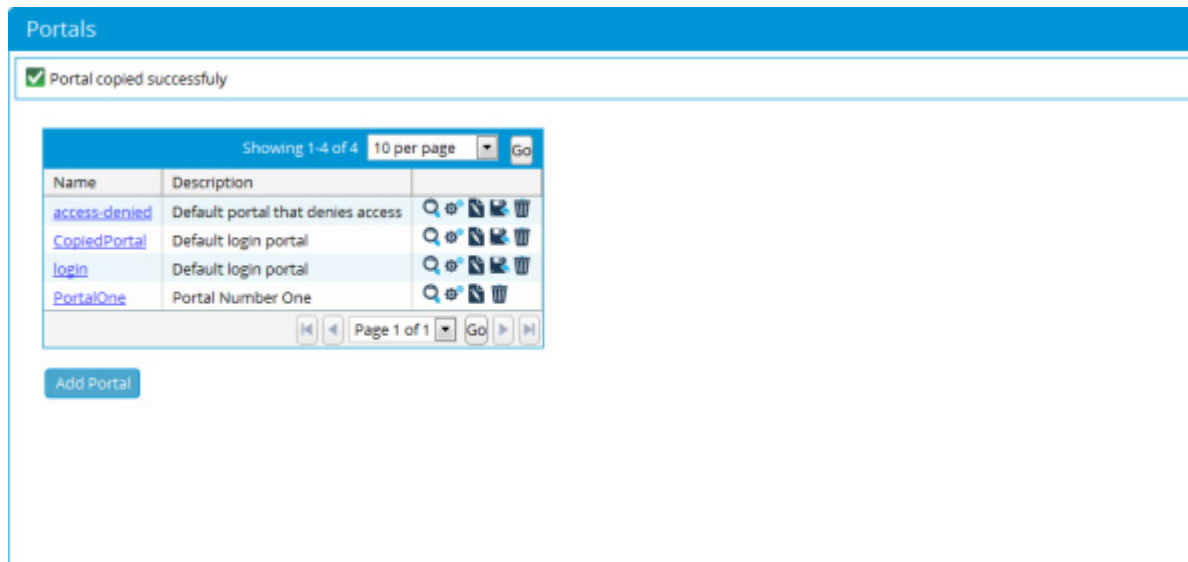
Copying a Portal



Click on the Copy Portal icon next to the portal that you have created



Enter your New Portal Name and then click on the Copy button, your portal will have been copied as shown below



4.

Creating a Portal Theme

In this chapter we take a look at how to Create a Portal Theme

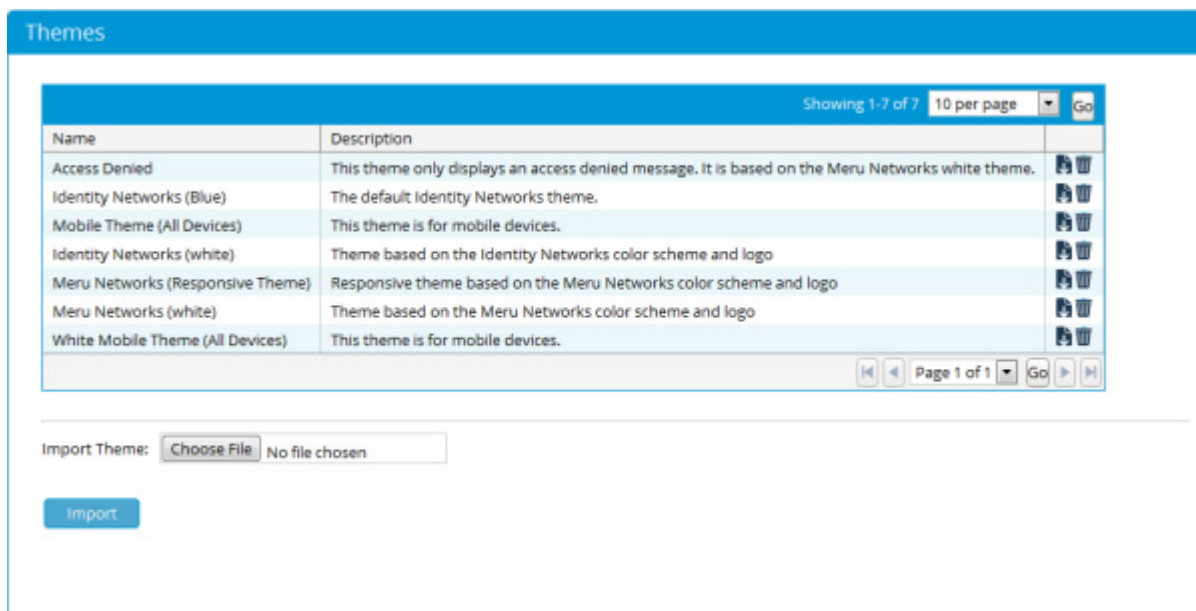
- The Sample Theme
 - The style.css file
 - The theme.xml file
 - ⑧ Name
 - ⑧ Description
 - ⑧ Author
 - ⑧ Preview
 - ⑧ Pages
 - ⑧ Images
 - ⑧ Colours
- Creating a Custom Theme

- Installing a Theme
- Available Widgets

The Default Themes

You can download any of the existing default themes that the FortiConnect provides to view its structure.

Log into the web admin user interface of the FortiConnect and browse to Guest Portals-->Themes and click on the export button next to 'The Default Fortinet Theme' as show below.



Unzip the default.zip file and confirm you have the following files :

- css/
 - style.css
- html/
 - °aup.html
 - login.html
 - password.html
 - payment.html
 - selfservice.html
 - success.html

- logout.html
- loggedOut.html
- images/
- theme.xml

The style.css file

This file should be placed in the css directory of the theme structure and should contain all the CSS styles that will be applied to the several HTML pages that make up the Portal site.

The theme.xml file

The theme.xml file list all resources used by the theme as well as defining the default values for several elements.

The file has 10 main elements:

1. Name
2. Public name
3. Description
4. Author
5. Preview
6. Pages
7. Optional pages
8. Navigation
9. Images
10. Colours
11. Scripts

Name

This is a mandatory element, it should only contain letters, digits and the underscore symbol, theme names are unique so if there is already a theme with this name installed on the FortiConnect you won't be able to install this theme.

Public Name

This is an optional element, it should contain the name displayed on the administration interface when referring to the theme, this element does not have the restrictions that apply to the name element.

If the `publicName` element is not present the theme internal name will be displayed.

Author

This attribute can be used by the theme author to place his name and/or contact details.

Preview

This attribute has two elements:

- small
- large

Both should have the name of two image files containing thumbnails for the theme, these are used by the hotspot setup pages to give the administrator an idea of how the hotspot will look if he chooses the theme. The recommended size for the small thumbnail is 200 pixels wide by 115 pixels tall and for the large thumbnail 800 pixels wide by 455 pixels tall. The files should be placed at the same level as the `theme.xml` file.

Pages

In the pages section of the theme.xml file you will list the HTML templates for every kind of page the Portal uses as well as declaring what content areas each page has and what should be it's default value.

A simple example would be:

```
<pages>
<login>
<file>login.html</file>
<components>
<component>
<tag>%TITLE%</tag>
<default>Login to the network</default>
</component>
<component>
<tag>%HEADER%</tag>
<default>Login to the network</default>
</component>
<component>
<tag>%MAIN%</tag>
<default/>
</component>
<component>
<tag>%FOOTER%</tag>
<default><![CDATA[Copyright &copy; yourcompany 2010]]></default>
</component>
</components>
<label>Login</label>
</login>
</pages>
```

The previous XML snippet tells us the HTML template for the login page is located at `html/login.html`, and on this page we have defined four components that the administrator users can customize with their content, we have also declared the default content for each component:

Table 1:

Component	Default Value
Title	Login to the network
Header	Login to the network
Main	
Footer	copyright © yourcompany 2010

If we open the `login.html` file with a text editor we can see where these components are used:

```
<h1>%HEADER%</h1>

<div class="main">%MAIN%</div>

<div class="widgetContainer">%LOGIN_WIDGET%</div>

<div id="navigation">%NAVIGATION_MENU%</div>

<div id="footer">%FOOTER%</div>
```

As we can see on the HTML the placeholder variables for the several components defined in `theme.xml` are placed amongst the markup, when the portal pages are generated the placeholders will be replaced with the content associated with them.

We can also see a few placeholders that weren't specified in the `theme.xml` file, these are:

- `%LOGIN_WIDGET%` - this will be replaced with the login widget if we were looking at the self service page template we should use `%SELF_SERVICE_WIDGET%` you can find a list of available widgets at the of this chapter.
- `%NAVIGATION_MENU%` - this will be replaced with a set of links to other pages available to users of the Portal.

The content of these placeholders is built dynamically by the FortiConnect depending on what options are selected during the Portal setup. When creating your own themes you should make sure that these placeholders are in your template files otherwise the Portal might not work as expected

Optional Pages

This section allows you to specify any optional pages you want to make available to portals using your theme. The default theme defines several optional pages, to add more you can copy one of the existing definitions and edit it as appropriate.

Navigation

Users can now add links to portal pages, to do this they have to add the following html:

```
<a %TAG%>this is a link</a>
```

%TAG% can be one of the following:

- %LINK_TO_LOGIN% - Link to the login page
- %LINK_TO_PMS% - Link to the pms login page
- %LINK_TO_PAYMENT% - Link to the Credit card payment page
- %LINK_TO_SELFSERVICE% - Link to the self service page
- %LINK_TO_PASSWORD% - Link to the password change page
- %LINK_TO_CLIENTCONFIGURATION% - Link to the smart connect page
- %LINK_TO_SUCCESS% - Link to the successful authentication page, this link will only work after successful authentication

To link to a optional page you should have a tag similar to

```
%LINK_TO_OPTIONAL_[PAGENAME]%
```

Where page name matches the name you gave the page on the theme.xml file so if in that file you have a generic page defined like:

```
<optionalPage menuItemWeight="10000">
<file>help.html</file>
<components>
<component>
<tag>%TITLE%</tag>
<default>Your title here</default>
</component>
<component>
<tag>%HEADER%</tag>
<default/>
</component>
```

```
<component>
<tag>%MAIN%</tag>
<default>Your content here</default>
</component>
<component>
<tag>%FOOTER%</tag>
<default><![CDATA[ &copy; 2011 Meru Networks. All Rights Reserved.]]></default>
</component>
</components>
<label>Help</label>
<name>help</name>
</optionalPage>
Your tag should be %LINK_TO_OPTIONAL_HELP%
```

Images

The images section of the theme.xml file should be used to list all image files that are referenced by the HTML and CSS for the theme.

When you open theme.xml and scroll down to the <images> section you will notice it is empty, you can add an image by replacing the <images/> tag with the following:

```
<images>
<image>
<label>Header image</label>
<description>Image placed on the header of the page</description>
<tag>%IMG_LOGO%</tag>
<file>Logo.png</file>
<dimensions>100x100</dimensions>
</image>
</images>
```

This snippet specifies the label, description and recommended dimensions for the image this information will be displayed on the Portal setup page so the administrator knows what this image is used for and can upload the right image for this purpose. The <tag> element specifies what placeholder variable will be used in HTML and CSS template files to reference this

particular image, the <file> element specifies which file is the default value for this image, this file should be placed in images/Logo.png.

To use this image in the login HTML template we could change the HTML to:

```
<div id="headerImage"></div>

<h1>%HEADER%</h1>

<div class="main">%MAIN%</div>

<div class="widgetContainer">%LOGIN_WIDGET%</div>

<div id="navigation">%NAVIGATION_MENU%</div>

<div id="footer">%FOOTER%</div>
```

If we wanted to reference this image on our CSS file, lets say as a background image we would have code like this:

```
.cssClass {
background-image:url( '%IMG_LOGO%' );
}
```

Colors

The colours section should contain a list of all customizable colours used in the theme.

The default theme already has a set of colours defined, to add a new one we would insert the following snippet between the <colour></colour> tags:

```
<colour>

<label>Default font colour</label>

<description/>

<tag>%CL_DEFAULT_FONT_COLOUR%</tag>

<value>#001844</value>

</colour>
```

This snippet specifies the label and description for the colour, this information will be displayed on the Portal setup page so the administrator knows where and what for the colour is used for. The <tag> element specifies what placeholder variable will be used in HTML and CSS template files to reference this colour, the <value> element specifies the colour hex value.

To use this colour in CSS we should have code like the following:

```
.cssClass {
color:%CL_DEFAULT_FONT_COLOUR%;
```

```
}
```

Scripts

The script section should contain a list of all javascript files you wish to use.

The default theme does not use any custom javascript files, to add a new javascript file we would insert the following snippet in the theme.xml file:

```
<scripts>
<script>
<tag>%JS_UTILS%</tag>
<value>utils.js</value>
</script>
</scripts>
```

The <tag> element specifies what placeholder variable will be used in HTML to reference this file, the <value> element specifies the file name, the file should be placed in the "js" directory at the root of the theme package. To include the code in utils.js on the html template files we should have code like the following:

```
<script type="text/javascript" src="%JS_UTILS%"></script>
```

Creating a custom theme

Now that we know what are the building blocks of a Portal theme we can use the default theme we downloaded to create our own theme.

Lets start by defining the requirements for our pages:

- Layout - Content displayed on the middle of the page, with three main areas that will be customizable by the administrator.
- Images - We will use two images one will be displayed on the page header and the other will be the favicon displayed on the browser address bar.
- Colours - We will define a background colour for the page and a different background colour for the main content area.

Start by editing the login.html template and modifying the HTML to suit your needs, in our case we should have something similar to:

```

<div id="content">
  <div id="header">
    <div id="headerImage"></div>
    <h1 class="pageTitle">%HEADER%</h1>
  </div>
  <div id="main">
    <div class="mainContent">%MAIN%</div>
    <div class="widgetContainer">%LOGIN_WIDGET%</div>
  </div>
  <div id="footer">
    <div id="navigation">%NAVIGATION_MENU%</div>
    <div class="copyright">%FOOTER%</div>
  </div>
</div>

```

You will need to copy any image files to the images/ directory.

The next step will be to edit the css/style.css file and define the styles that we will apply to the HTML markup we defined previously. The following code would implement the layout we proposed:

```

body{
  font-family:Arial;
  background-color:#333333;
}
#content{d width:45%;
  margin:auto;
  padding:20px;
  margin-top:50px;
  background-color:#eeeeee;
}
#header{
  text-align:center;
  margin-bottom:25px;

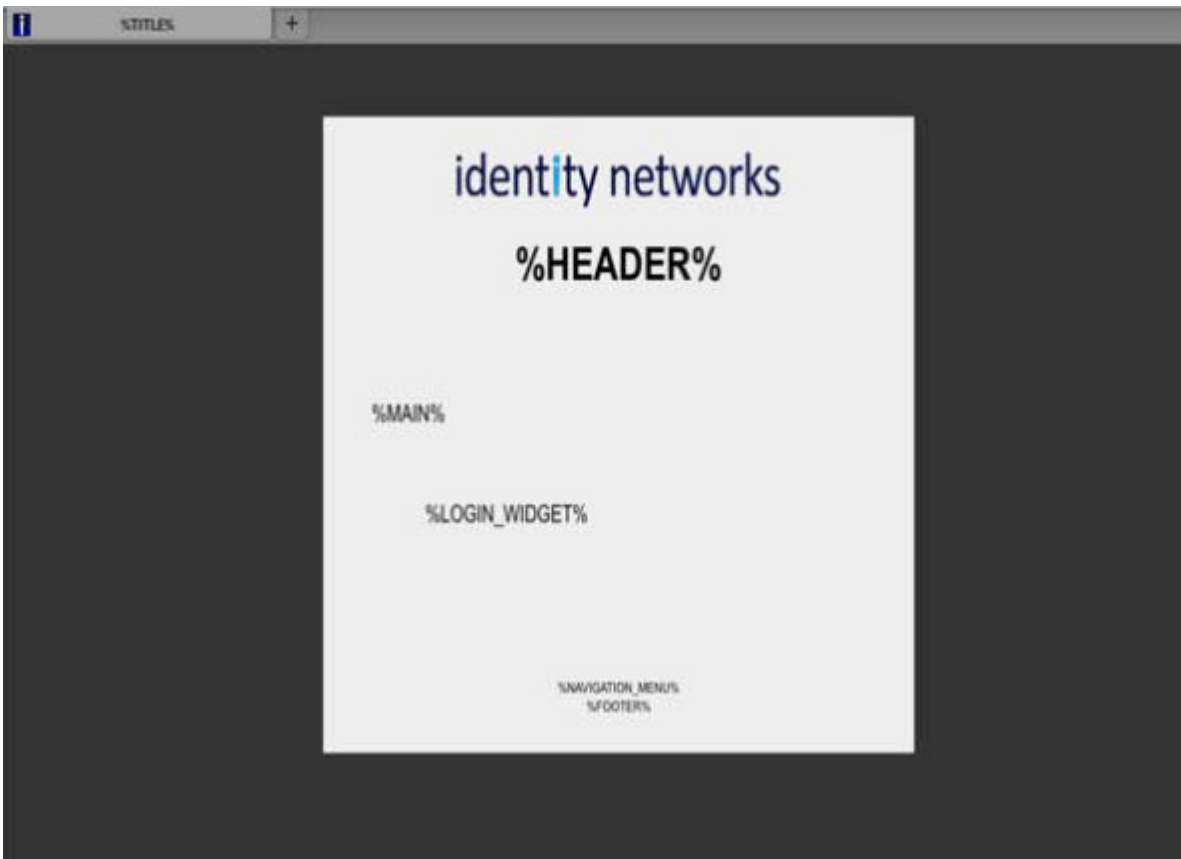
```

Creating a custom theme

```
padding:5px;
}
#main{
padding:25px;
}
.widgetContainer {
width:80%;
padding:50px; }
#footer{
text-align:center;
margin-top:25px;
padding:5px;
font-size:x-small;
}
.navigation{
padding:5px;
}
```

Again you will notice that the actual colour values are used in this file instead of placeholders, this allows us to view the page in the browser while we develop the design of our pages.

If you open the login.html file in your browser you will see something like:



You can also replace the placeholders visible on the body of the page with dummy content to get a better feel of how it would look on your page, this is also useful to take preview screenshots to include in your theme package.

Once you are happy with the layout, its time to update the theme.xml, so all elements that are customizable by the administrator are declared, in our case the file would look similar to:

```
<?xml version="1.0"?>
<hotspotTheme>
  <name>sample_theme</name>
  <description>plain theme</description>d<author></author>d  <preview>d
    <small>thumb.png</small>d  <large>preview.png</large>d  </preview>
  <pages>
    <login>
      <file>login.html</file>
    <components>
```

```
<component>
  <tag>%TITLE%</tag>
  <default>Login to the network</default>
</component>
<component>
  <tag>%HEADER%</tag>
  <default>Login to the network</default>
</component>
<component>
  <tag>%MAIN%</tag>
  <default/>
</component>
<component>
  <tag>%FOOTER%</tag>
  <default><![CDATA[Copyright &copy; yourcompany 2010]]></default>
</component>
</components>
<label>Login</label>
</login>
<selfService>
  <file>selfservice.html</file>
  <components>
    <component>
      <tag>%TITLE%</tag>
      <default>Login to the network</default>
    </component>
    <component>
      <tag>%HEADER%</tag>
      <default>Create your guest account</default>
    </component>
  </components>
</selfService>
```



```

    </component>
    <component>
        <tag>%MAIN%</tag>
        <default/>
    </component>
    <component>
        <tag>%FOOTER%</tag>
        <default><![CDATA[Copyright &copy; yourcompany 2010]]></default>
    </component>
</components>
<label>Self Service</label>
</selfService>
<payment>
    <file>payment.html</file>
    <components>
        <component>
            <tag>%TITLE%</tag>
            <default>Login to the network</default>
        </component>
        <component>
            <tag>%HEADER%</tag>
            <default>Purchase your account</default>
        </component>
        <component>
            <tag>%MAIN%</tag>
            <default/>
        </component>
        <component>
            <tag>%FOOTER%</tag>

```

```

        <default><![CDATA[Copyright &copy; yourcompany 2010]]></default>
    </component>
</components>
<label>Purchase Account</label>
</payment>
<password>
    <file>password.html</file>
    <components>
        <component>
            <tag>%TITLE%</tag>
            <default>Login to the network</default>
        </component>
        <component>
            <tag>%HEADER%</tag>
            <default>Change your password</default>
        </component>
        <component>
            <tag>%MAIN%</tag>
            <default/>
        </component>
        <component>
            <tag>%FOOTER%</tag>
            <default><![CDATA[Copyright &copy; yourcompany 2010]]></default>
        </component>
    </components>
<label>Change Password</label>
</password>
<aup>
    <file>aup.html</file>

```

```

<components>
  <component>
    <tag>%TITLE%/tag>
    <default>Login to the network</default>
  </component>
  <component>
    <tag>%HEADER%/tag>
    <default>Acceptable Usage Policy</default>
  </component>
  <component>
    <tag>%MAIN%/tag>
    <default>By clicking "Accept" you agree to the terms and
      conditions.....</default>
  </component>
  <component>
    <tag>%FOOTER%/tag>
    <default><![CDATA[Copyright &copy; yourcompany 2010]]></default>
  </component>
</components>
<label>Acceptable Usage Policy</label>
</aup>
<generic>
  <file>generic.html</file>
  <components>
    <component>
      <tag>%TITLE%/tag>
      <default>Login to the network</default>
    </component>
    <component>
      <tag>%HEADER%/tag>

```

Creating a custom theme

```
<default/>

</component>

<component>

  <tag>%MAIN%</tag>

  <default>your text here</default>

</component>

<component>

  <tag>%FOOTER%</tag>

  <default><![CDATA[Copyright &copy; yourcompany 2010]]></default>

</component>

</components>

<label>Generic page</label>

</generic>

</pages>

<images>

  <image>

    <label>Header image</label>

    <description>Image placed on the header of every page</description>

    <tag>%IMG_LOGO%</tag>

    <file>Logo.png</file>

    <dimensions>100x100</dimensions>

  </image>

  <image>

    <label>Favicon</label>

    <description>Image to be displayed in browser address bar</description>

    <tag>%IMG_FAV_ICON%</tag>

    <file>Favicon16.ico</file>

    <dimensions>16x16</dimensions>

  </image>
```

```

</images>
<colours>
  <colour>
    <label>Body background color</label>
    <description/>
    <tag>%CL_BODY_BACKGROUND%</tag>
    <value>#333333</value>
  </colour>
  <colour>
    <label>Content area background color</label>
    <description/>
    <tag>%CL_CONTENT_BACKGROUND%</tag>
    <value>#eeeeee</value>
  </colour>
</colours>
</hotspotTheme>

```

Since we are using the same customizable areas we didn't make any changes to the <pages> element content, it is generally a good idea to use the same names for the content areas e.g. % HEADER%, %FOOTER%, etc... as this will allow users to switch between themes using the content they have defined already.

Now that we have updated the theme.xml and we are happy with the design of our page we should replace any colour and image references with their respective placeholder on both the login.html file and the style.css file.

The login html file should look similar to :

```

<div id="content">
  <div id="header">
    <div id="headerImage"></div>
    <h1 class="pageTitle">%HEADER%</h1>
  </div>
  <div id="main">
    <div class="mainContent">%MAIN%</div>
  </div>
</div>

```

Creating a custom theme

```
<div class="widgetContainer">%LOGIN_WIDGET%/div>
</div>
<div id="footer">
  <div id="navigation">%NAVIGATION_MENU%/div>
  <div class="copyright">%FOOTER%/div>
</div>
</div>
```

The style.css file should look similar to:

```
body{
  font-family:Arial;
  background-color:%CL_BODY_BACKGROUND%;
}
#content{
  width:45%;
  margin:auto;
  padding:20px;
  margin-top:50px;
  background-color:%CL_CONTENT_BACKGROUND%;
}
#header{
  text-align:center;
  margin-bottom:25px;
  padding:5px;
}
#main {
  padding:25px;
}
.widgetContainer {
  width:80%;
  padding:50px;
}
#footer{
  text-align:center;
```

```

margin-top:25px;
padding:5px;
font-size:x-small;
}
.navigation{
padding:5px;
}

```

In this case we want all pages to have the same basic layout, so we need edit the remaining files in the `html/` directory and replace their contents with the code from `login.html`, the only change we need to do is replace the `%LOGIN_WIDGET%` placeholder with the relevant widget for the page in question, the following code would be present in the `selfservice.html` file:

```

<div id="content">
  <div id="header">
    <div id="headerImage"></div>
    <h1 class="pageTitle">%HEADER%</h1>
  </div>
  <div id="main">
    <div class="mainContent">%MAIN%</div>
    <div class="widgetContainer">%SELF_SERVICE_WIDGET%</div>
  </div>
  <div id="footer">
    <div id="navigation">%NAVIGATION_MENU%</div>
    <div class="copyright">%FOOTER%</div>
  </div>
</div>

```

Now that the HTML and CSS files are done we need to give our theme a name and description, declare our preview images and fill in the author information in `theme.xml`.

Assuming we took two screenshots of our page, `preview_small.png` and `preview_large.png` and placed these files in the root directory of our theme we should edit the `theme.xml` file to look similar to:

```

<?xml version="1.0"?>
<hotspotTheme>
  <name>tutorial_theme</name>

```

Creating a custom theme

```
<description>Simple theme built during the tutorial</description>
<author>myname</author>
<preview>
  <small>preview_small.png</small>
  <large>preview_large.png</large>
</preview>
<pages>
  <login>
    <file>login.html</file>
    <components>
      <component>
        <tag>%TITLE%</tag>
        <default>Login to the network</default>
      </component>
      <component>
        <tag>%HEADER%</tag>
        <default>Login to the network</default>
      </component>
      <component>
        <tag>%MAIN%</tag>
        <default/>
      </component>
      <component>
        <tag>%FOOTER%</tag>
        <default><![CDATA[Copyright &copy; yourcompany 2010]]></default>
      </component>
    </components>
    <label>Login</label>
  </login>
  <selfService>
```



```

<file>selfservice.html</file>
<components>
  <component>
    <tag>%TITLE%</tag>
    <default>Login to the network</default>
  </component>
  <component>
    <tag>%HEADER%</tag>
    <default>Create your guest account</default>
  </component>
  <component>
    <tag>%MAIN%</tag>
    <default/>
  </component>
  <component>
    <tag>%FOOTER%</tag>
    <default><![CDATA[Copyright &copy; yourcompany 2010]]></default>
  </component>
</components>
<label>Self Service</label>
</selfService>
<payment>
  <file>payment.html</file>
  <components>
    <component>
      <tag>%TITLE%</tag>
      <default>Login to the network</default>
    </component>
    <component>

```

Creating a custom theme

```
<tag>%HEADER%</tag>

<default>Purchase your account</default>

</component>

<component>

  <tag>%MAIN%</tag>

  <default/>

</component>

<component>

  <tag>%FOOTER%</tag>

  <default><![CDATA[Copyright &copy; yourcompany 2010]]></default>

</component>

</components>

<label>Purchase Account</label>

</payment>

<password>

  <file>password.html</file>

  <components>

    <component>

      <tag>%TITLE%</tag>

      <default>Login to the network</default>

    </component>

    <component>

      <tag>%HEADER%</tag>

      <default>Change your password</default>

    </component>

    <component>

      <tag>%MAIN%</tag>

      <default/>

    </component>

  </components>

</password>
```

```

    <component>
        <tag>%FOOTER%</tag>
        <default><![CDATA[Copyright &copy; yourcompany 2010]]></default>
    </component>
</components>
<label>Change Password</label>
</password>
<aup>
<file>aup.html</file>
<components>
    <component>
        <tag>%TITLE%</tag>
        <default>Login to the network</default>
    </component>
    <component>
        <tag>%HEADER%</tag>
        <default>Acceptable Usage Policy</default>
    </component>
    <component>
        <tag>%MAIN%</tag>
        <default>By clicking "Accept" you agree to the terms and
            conditions.....</default>
    </component>
    <component>
        <tag>%FOOTER%</tag>
        <default><![CDATA[Copyright &copy; yourcompany 2010]]></default>
    </component>
</components>
<label>Acceptable Usage Policy</label>
</aup>

```

Creating a custom theme

```
<generic>
  <file>generic.html</file>
  <components>
    <component>
      <tag>%TITLE%</tag>
      <default>Login to the network</default>
    </component>
    <component>
      <tag>%HEADER%</tag>
      <default/>
    </component>
    <component>
      <tag>%MAIN%</tag>
      <default>your text here</default>
    </component>
    <component>
      <tag>%FOOTER%</tag>
      <default><![CDATA[Copyright &copy; yourcompany 2010]]></default>
    </component>
  </components>
  <label>Generic page</label>
</generic>
</pages>
<images>
  <image>
    <label>Header image</label>
    <description>Image placed on the header of every page</description>
    <tag>%IMG_LOGO%</tag>
    <file>Logo.png</file>
```

```

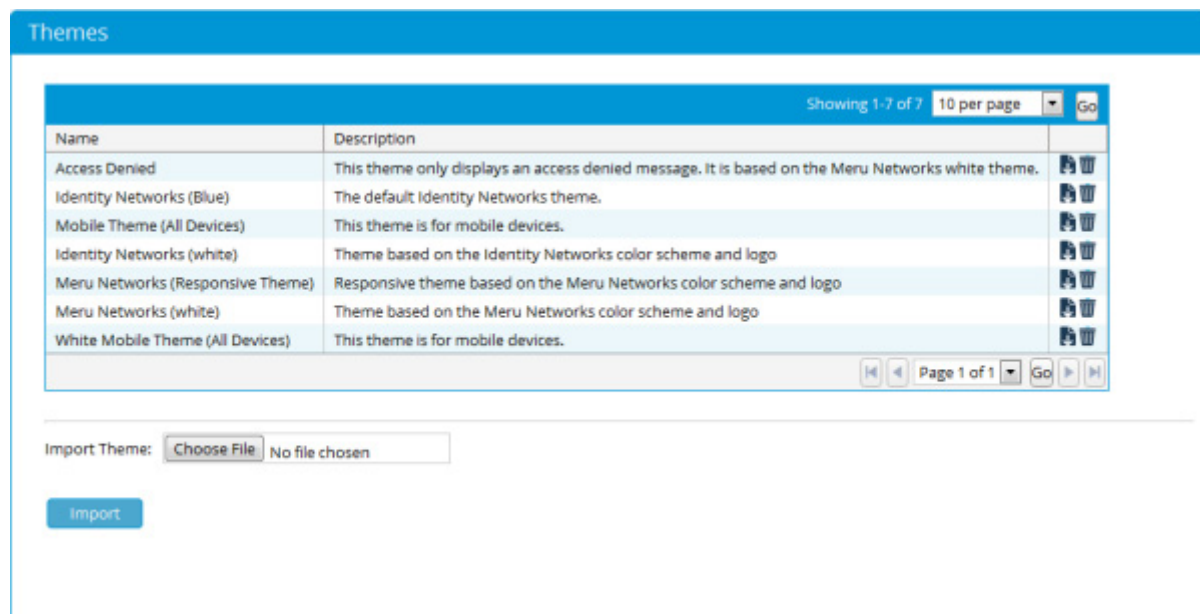
    <dimensions>100x100</dimensions>
</image>
<image>
    <label>Favicon</label>
    <description>Image to be displayed in browser address bar</description>
    <tag>%IMG_FAV_ICON%</tag>
    <file>Favicon16.ico</file>
    <dimensions>16x16</dimensions>
</image>
</images>
<colours>
    <colour>
        <label>Body background color</label>
        <description/>
        <tag>%CL_BODY_BACKGROUND%</tag>
        <value>#333333</value>
    </colour>
    <colour>
        <label>Content area background color</label>
        <description/>
        <tag>%CL_CONTENT_BACKGROUND%</tag>
        <value>#eeeeee</value>
    </colour>
</colours>
</hotspotTheme>

```

The final step is to create a zip file containing all the theme files, the directory structure of the zip file should be similar to that of the default theme.

Installing a Theme

To install a theme go to the Guest Portals --> Themes from the Administration interface.



Click the Choose File button and browse your computer for the theme file, after selecting the file click the Import button and verify the page is refreshed and the new theme is present in the Themes list.

Available Widgets

Table 2:

Page	Widget
Login	%LOGIN_WIDGET%
Payment	%PAYMENT_WIDGET%
Self Service	%SELF_SERVICE_WIDGET%
Acceptable Usage Policy	%AUP_WIDGET%
Password Change	%PASSWORD_WIDGET%
Logout	%LOGOUT_WIDGET%
Logout Popup	%LOGOUT_POPUP%
Time Left	%TIME_LEFT_WIDGET%

Portal Rules

The FortiConnect can be used to create a set of Portal Rules for redirecting Users to different Portals that have been created.

From the FortiConnect Administration interface go to Guest Portals --> Portal Rules as shown below.

Portal Rules

Portal Rules

Each rule is checked in the following order. If a rule is matched the guest is directed to the rule's portal (or is denied access) and no other rules are checked. If no rule matches the default rule is applied.

Set your network devices to redirect to the following URL to use portal rules:

https://{MERU_CONNECT}/portal/{DEVICE_IP}

Order	Name	Description	Rule	Portal	Hit Count	
1	Default	Default if no other rules match		login	0	

[Test portal rules](#)

Save

Cancel

Add Rule

Each rule that is created is checked in the order shown. If a rule is matched, the User is directed to the rules portal (or denied access) and no other rules are checked. If no rule matches then the default rule is applied.

Note: FortiConnect comes with the Default rule.

1. To add a rule click on the Add Rule button.

Edit Rule

Guests are directed to the specified portal if all the specified conditions are met.

Rule Name:

Rule Description:

equal to

Rule Action:
☒ Go to portal

☐ No portal (sends HTTP 403 Unauthorised header)

2. In the fields provided input the following -
 - Rule Name - Create a name for your rule.
 - Rule Description - Enter a description for your rule.
 - Rule Action - Check the Go To Portal option and then use the drop down menu to select from one of the portals you have created, or one of the default portals, to direct the User to the relevant portal. Check No portal if you do not wish to redirect the User.
3. From the drop down lists provided create a set of rules that applies to your portal. The example that has been created above reflects Users using 'Mobile' as their device, you will see that the Rule Action has been set to Go To Portal'mobile'. Therefore any Users using a mobile device will be directed to a portal is designed for mobile users.
4. Click add condition once created.
5. Click Save to complete.

Portal Rules




Portal Rules

✓ Portal rule saved

Each rule is checked in the following order. If a rule is matched the guest is directed to the rule's portal (or is denied access) and no other rules are checked. If no rule matches the default rule is applied.

Set your network devices to redirect to the following URL to use portal rules:

https://{MERU_CONNECT}/portal/{DEVICE_IP}

Order	Name	Description	Rule	Portal	Hit Count	
1	Rule One	test	idm-host-ip-address equals 10.10.1.1	access-denied	0	 
2	Default	Default if no other rules match		login	0	

[Test portal rules](#)

[Save](#) [Cancel](#) [Add Rule](#)

As you can see the rule has now been created and added to the list.

- Use the up and down arrow icons next to the order number to move the order of the rules. Click on Add Rule to create any further rules.
- You can test any portal rules you have created by clicking on the Test Portal Rules link, this will display a screen as shown below.

Test Portal Rules

This finds the rule that matches the environment you define below.

Browser: Chrome 12.0 on Windows [Detect my browser](#)

Mobile device: ☐

Browser Language: English

Time: 11:07:00 on Tuesday in America/Los_Angeles [Now](#)

RADIUS Client IP Address:

User IP Address: 192.168.137.1

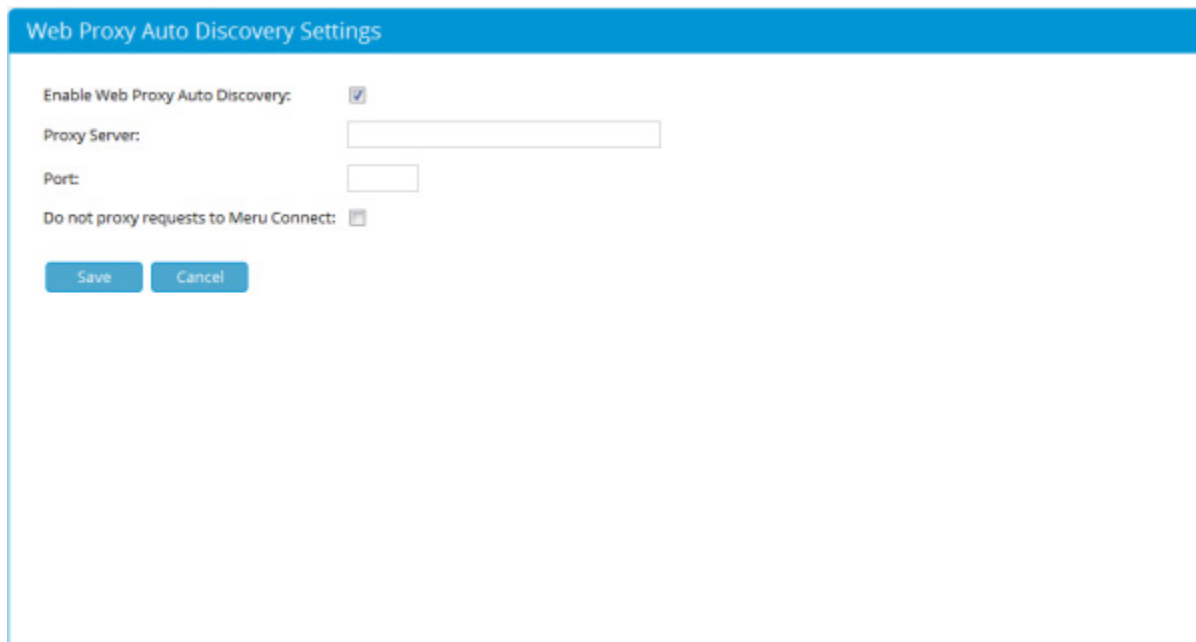
Meru Connect IP Address: 192.168.137.20

[Find Matching Rule](#) [Back to Rules](#)

8. Find any rule that matches the environment you define :-
 - Browser - From the drop down menu's select and define the browser you wish to test against.
 - Mobile Device - Check if using a mobile device.
 - Browser Language - From the drop down menu select the browser language.
 - Time - From the drop down menu's select a time you wish to test.
 - RADIUS Client IP Address - Enter the RADIUS Clients IP address.
 - User IP Address - Enter the User's IP Address.
 - FortiConnect IP Address - Enter the FortiConnects IP Address.
9. Click on Find Matching Rule to test.

Proxy Auto Discovery

Administrators can host Web Proxy Auto Discovery PAC files on the FortiConnect, to do this go to Guest Portals --> Proxy Auto Discovery as shown in the screen shot below.



The image shows a 'Web Proxy Auto Discovery Settings' dialog box. It has a blue header bar with the title. Below the header, there are four settings: 'Enable Web Proxy Auto Discovery' with a checked checkbox, 'Proxy Server' with a text input field, 'Port' with a text input field, and 'Do not proxy requests to Meru Connect' with an unchecked checkbox. At the bottom left, there are two buttons: 'Save' and 'Cancel'.

1. Check the Enable Web Proxy Auto Discovery check box.
2. Enter the Proxy Server settings in the field provided.
3. Enter the Port number in the field provided.
4. Check the Do not proxy requests to FortiConnect if you wish to do so.
5. Click on Save to continue.

Hosted Files

FortiConnect supports the uploading of arbitrary files for use in Portals.

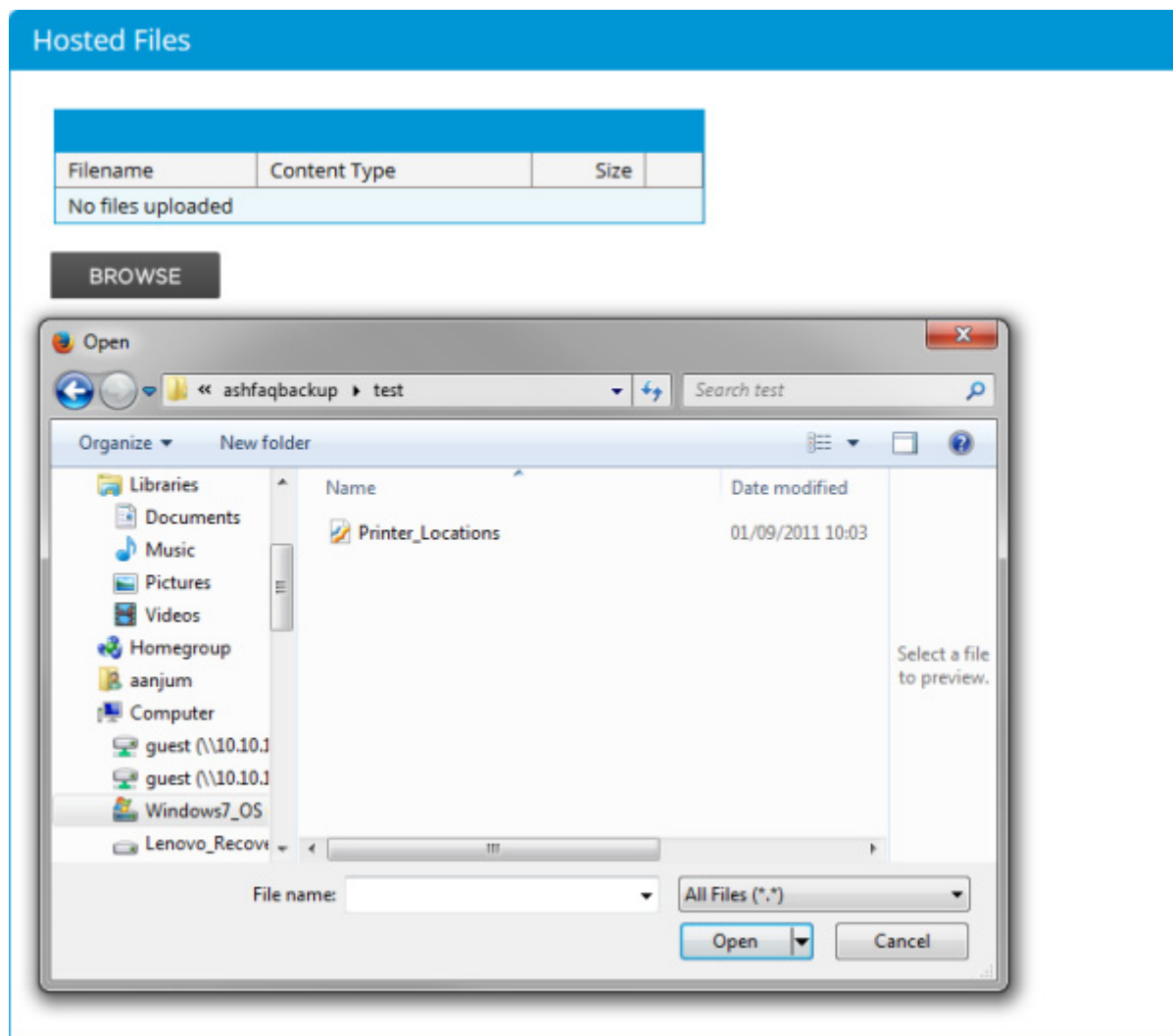
To upload any files, go to Guest Portals-->Hosted Files on the FortiConnect Administration interface as shown below.

Hosted Files

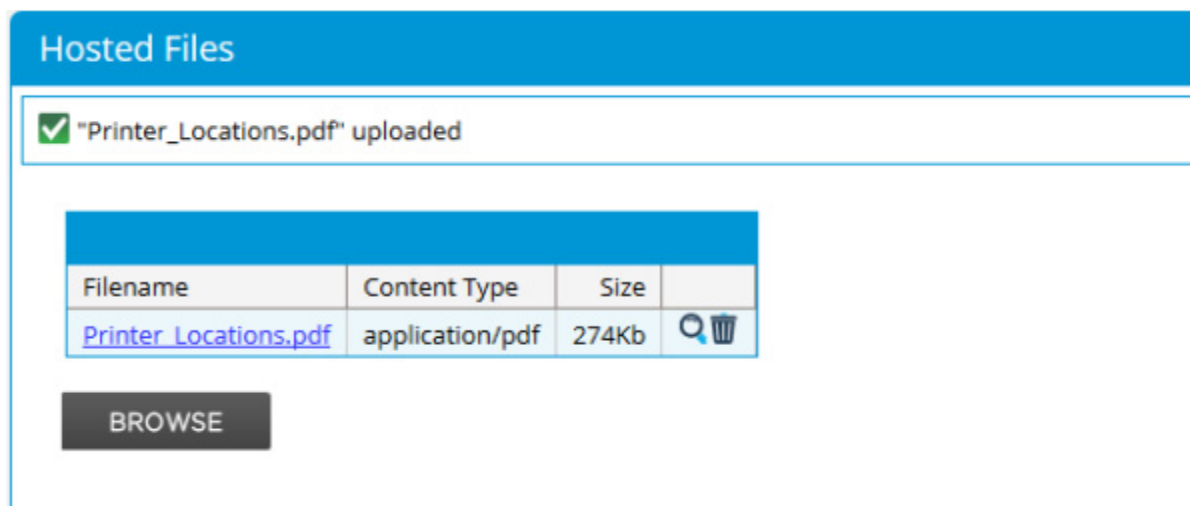
Filename	Content Type	Size	
No files uploaded			

BROWSE

1. To upload a file click on the BROWSE button to locate the file you wish to upload for use in a Portal as shown below.



2. Select the file you wish to upload and click on Save, the file will then be displayed as shown below.



3. To view the file click on the magnifying glass icon.
4. To delete a file click on the bin icon.

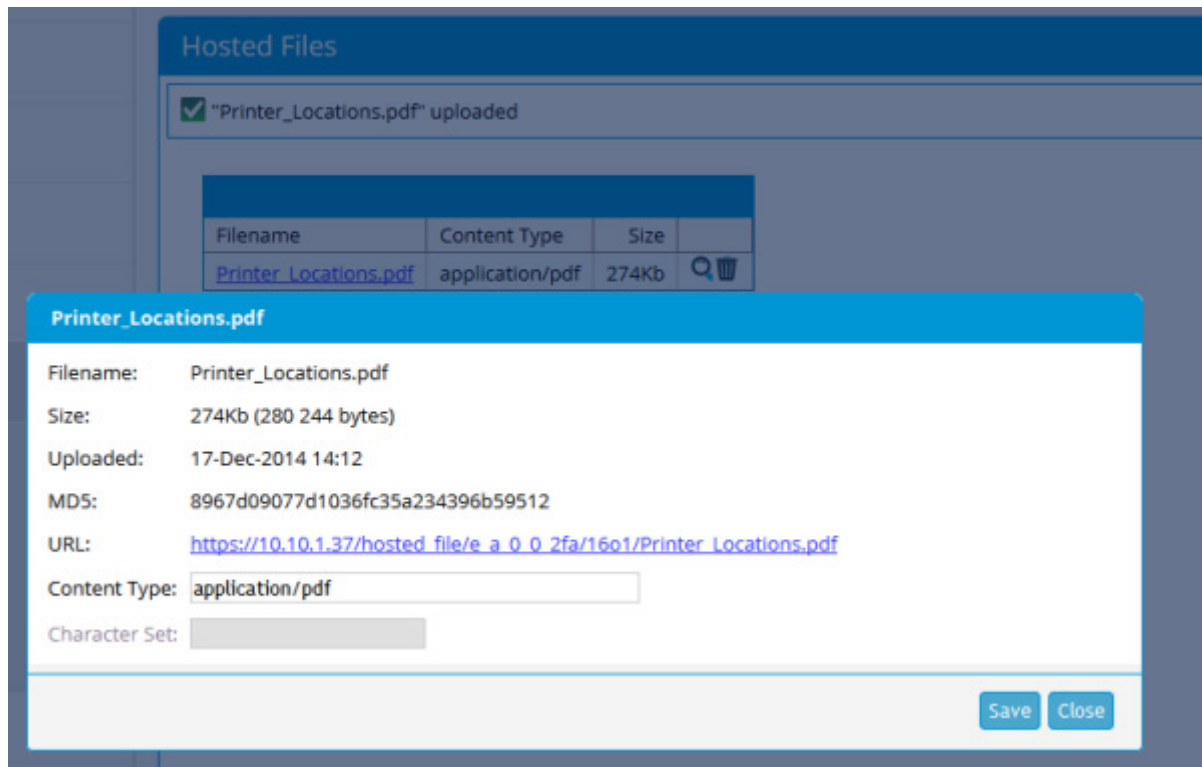
Adding links to Portals

To add your link to a page in your Portal, we can follow the instructions below.

Note: For this example we will add to the Login Page on the Portal using pre authentication, steps and screen shots for other pages will differ.

Go to Guest Portals-->Hosted Files on the FortiConnect Administration interface.

1. Click on the Filename of the link you wish to add to your page as shown below.



2. Copy the URL of the link you wish to use for your Portal and click on close.
3. Go to Guest Portals-->Portals on the FortiConnect Administration interface.
4. Click on the Edit Portal Content Icon next to the Portal you wish to add the link to, and identify which area on the Portal you wish have the link displayed.

Login Page

Cookies Instructions Page

Close this window Page

Authenticating waiting Page

Session management Page

Login Page

Acceptable Usage Policy Page

Purchase Account Page

Successful Authentication Page

Logout Page

Logged Out Page

Client Configuration Page

IOS auto login Page

Widget Labels

Customise the content of the Login page

Page label:

Header:

Main:

Title:

5. Copy the Link into the appropriate area and wrap it with Standard HTML Anchor Tags.
6. Click Save

Hotel Property Management System Integration

FortiConnect supports integration with a number of Hotel Property Management Systems. FortiConnect allows communication with the Hotel Property Management System to enable billing for internet access direct to a guest's hotel room bill. This is achieved by adding a Hotel Property Management System login widget to a portal which will communicate with the Hotel Property Management System.

Different Hotel Property Management Systems can be added via the Admin Interface > Guest Portals > Hotel PMS.

Supported Hotel Property Management System's include:-

- HOBIC (via TCP/IP)
- MICROS Fidelio Suite / Opera (via TCP/IP)
- Infoden RMS
- Control Lodging Link (via TCP/IP) - a list of support Hotel Property Management Systems are available here <http://www.comtrol.com/pub/en/Property-Management-Systems-Partners>

Each Portal will be able to define it's own access plans which determine the access time allowed and associated charge to be posted to the Hotel Property Management System configured for that portal.

The first time a user goes to the portal and supplies their credentials (these can be last name and room number, username and password, etc) they will be taken to a page with the available access plans, once the user select ones and proceeds with the authentication process their room will be charged.

The user will be able to login without being charged until their account expires, once the account expires the user will be again taken to the access plan selection where they can purchase more time on the network.

Ordering and Support with PMS Vendors

Some PMS vendors require additional part numbers to be ordered to allow integration, please check with the vendor you wish to integrate with before ordering.

- For support with Opera PMS, the following part number needs to be ordered from Micros

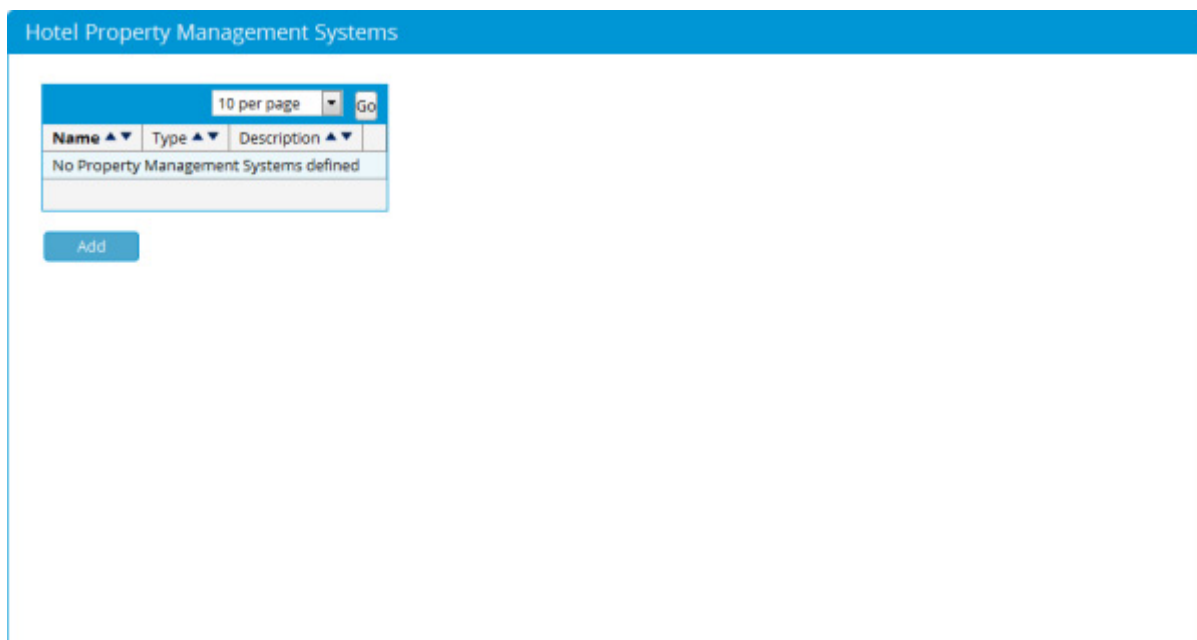
What Part Numbers Do I Need?

Part No	Product ID (FKT)	Description
IO-5009-271	IFC_IMN	Identity Manager by Meru Networks

Adding a Hotel Property Management System

To add a Hotel Property Management System from the administration interface:

1. Select Guest Portals > Hotel PMS as shown below.



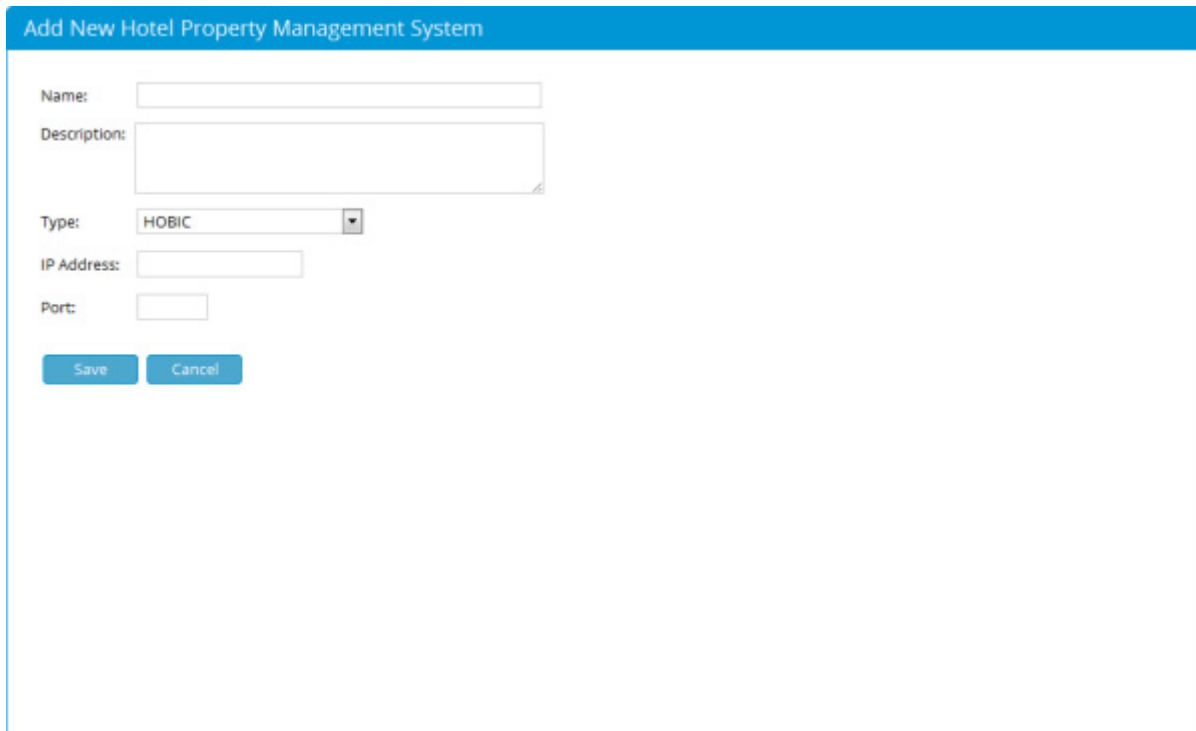
Hotel Property Management Systems

10 per page Go

Name ▲▼	Type ▲▼	Description ▲▼
No Property Management Systems defined		

Add

2. Click the Add button



The screenshot shows a web form titled "Add New Hotel Property Management System" with a blue header bar. The form contains the following fields and controls:

- Name:** A single-line text input field.
- Description:** A multi-line text area.
- Type:** A dropdown menu with "HOBIC" selected.
- IP Address:** A single-line text input field.
- Port:** A single-line text input field.
- Buttons:** Two buttons labeled "Save" and "Cancel" are located at the bottom left of the form.

3. Fill in the appropriate fields to add the Hotel Property Management System :-
 - Name - Name of the Hotel Property Management System
 - Description - Description of the Hotel Property Management System.
 - Type - From the drop down menu select the type of Hotel Property Management System you will integrate with.
 - IP Address - Enter the IP address of the Hotel Property Management System.
 - Port - Enter the Port Number required for the Hotel Property Management System.
4. Click on Save once complete.

Editing and Deleting a Hotel Property Management System

5. To Edit an existing Hotel Property Management System go to Guest Portals --> Hotel PMS as shown below

Hotel Property Management Systems

Showing 1-1 of 1

10 per page

Go

Name ▲▼	Type ▲▼	Description ▲▼	
PMS One	HOBIC	Test PMS	

Page 1 of 1

Go

Add

- Click on the link of the Hotel Property Management System you wish to edit

Edit Hotel Property Management System

Name:

Description:

Type:

IP Address:

Port:

Save

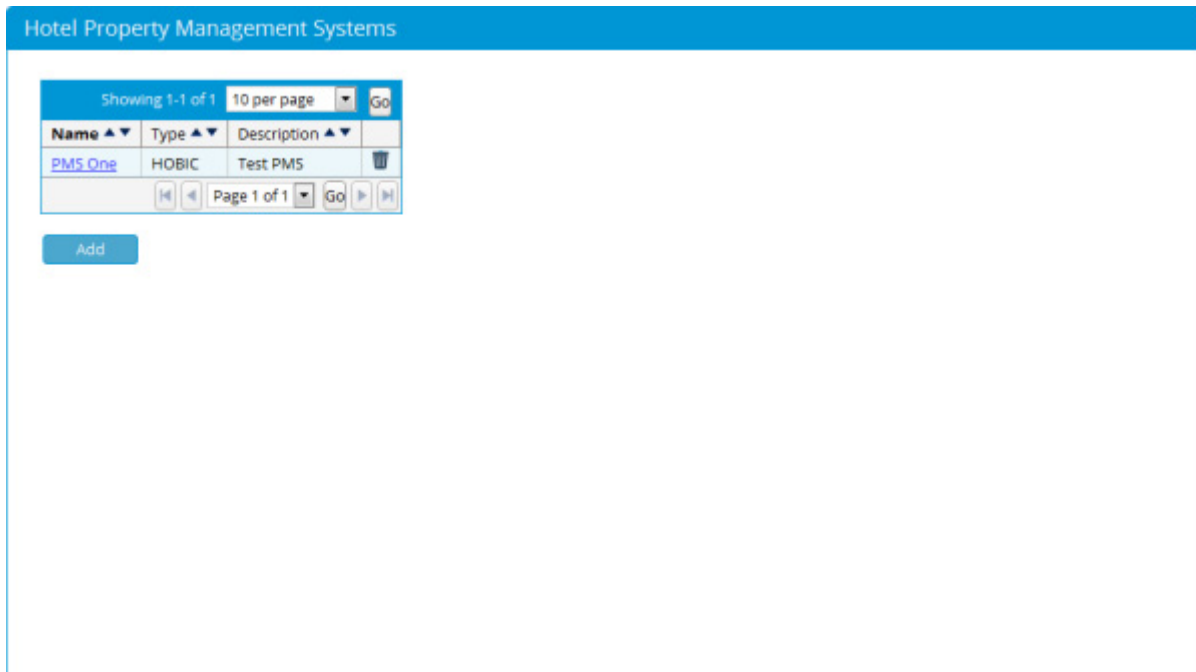
Cancel

- Fill in the appropriate fields to edit the Hotel Property Management System :-
 - Name - Name of the Hotel Property Management System
 - Description - Description of the Hotel Property Management System.

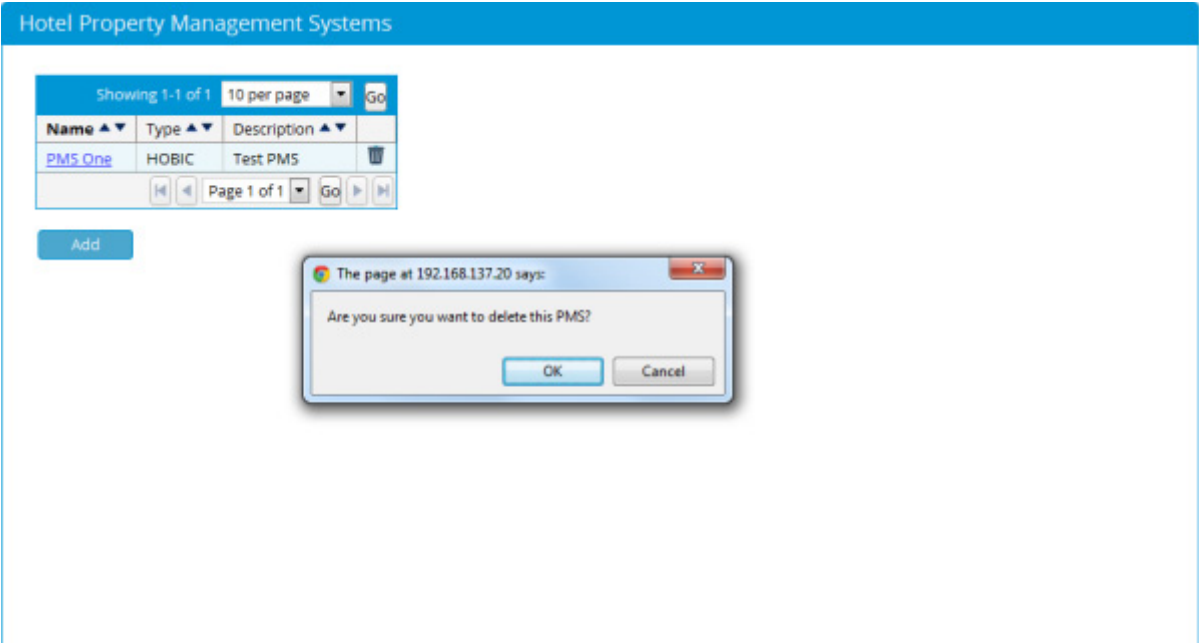
- **Type** - From the drop down menu select the type of Hotel Property Management System you will integrate with.
- **IP Address** - Enter the IP address of the Hotel Property Management System.
- **Port** - Enter the Port Number required for the Hotel Property Management System.

Click on Save once complete.

8. To delete a Hotel Property Management System go to Guest Portals --> Hotel PMS as shown below



9. Click on the Bin icon to the right of the Hotel Property Management System you wish to delete and click on yes to confirm as shown below.



PMS Payment Reports

Administrators can run a Payment Report which details all transactions purchased through a Property Management Systems account.

1. From the Admin UI Interface, go to Reports & Logs-->Payments Report, you will be presented with a screen similar to the one below.

Payments Report

Payment Method: Payment Provider:

Portal: Access Plan:

Transaction ID: From:

Username: To:

Name on Card:

Purchased Guest Accounts Summary

Portal	Number of Accounts	Total
No Records Found		

Transaction ID ▲▼	Name on Card ▲▼	Portal ▲▼	Payment Provider ▲▼	Access Plan	Username ▲▼	Amount ▲▼	Date ▲▼
No Records Found							

10 per page

2. To run a report on PMS Billing select the PMS Billing option from the Payment Method field :-
 - Hotel PMS - From the drop down menu select a Hotel PMS.
 - Portal - From the drop down menu select a Portal.
 - Access Plan - From the drop down menu select an access plan.
 - Transaction ID - From the drop down menu select a Transaction ID.
 - Username - From the drop down menu select a Username.
 - Customer Name - From the drop down menu select a Customer Name.
 - Room Number - From the drop down menu select a Room Number.
 - From - From the drop down menu select a From Date.
 - To - From the drop down menu select a To Date.
3. Click Run to display the report on screen, or click Download CSV to download as a file to your desktop.
4. A detailed report will show.
 - Transaction ID - Guests Transaction ID
 - Name on Card - Guests name on card provided.

- Portal - Portal the Guest accessed.
- Guest - Guest account username.
- Payment Provider - Which Payment Provider the Guest used.
- Access Plan - Access plan the Guest used for Guest access.
- Username - Username of the Guest.
- Amount - Amount the Guest was charged.
- Date - Date and Time the Guest user accessed.

Credit Card Billing

Configuring Payment Providers for Credit Card Billing

When using the FortiConnect to allow Users to purchase accounts using credit card billing, you need to add the details of the payment provider. The payment provider details are needed to allow your payment provider to perform credit card billing into your account.

Adding a Payment Provider

From the administration interface, select Guest Portals > Payment Providers as shown below.

Adding a Payment Provider

Payment Providers

10 per page

Go

Name ▲▼	Type ▲▼	Description ▲▼	
No payment providers defined			

Add

1. Click Add and enter the relevant details in the fields as shown below.

2. Enter the details as follows:

- **Account Name**—Enter the name of the payment provider account.
- **Account Description**—Enter the description of the payment provider account.
- **Payment Provider**—Choose the relevant payment provider from the dropdown menu provided.
- **Operation Mode** - From the dropdown menu select whether this will be a production or test payment gateway. The link to the right shows the URL that will be used for the payment gateways API.
- **API Login**—Enter the API login for the payment provider account.
- **Transaction Key**—Enter the transaction key for the payment provider account.
- From the **Available Cards** list, select the cards you wish to allow for transactions and click the relevant arrows to add or remove them.
- You can test your connection and send a test transaction by clicking on the **Test Connection** button.

3. In the **Payment Page Settings** section, you can show or hide the input fields on the payment page of the Portal, determine whether you wish use each field using the drop down menu -

- **Required** - Field requires input

Adding a Payment Provider

- Optional - Field can be left blank
- Unused - Field will not appear

4. Once completed, click the Save button.

Selecting a different payment provider will enable more or less options depending on the payment provider settings required, this is shown below using Payflow Pro as an example.

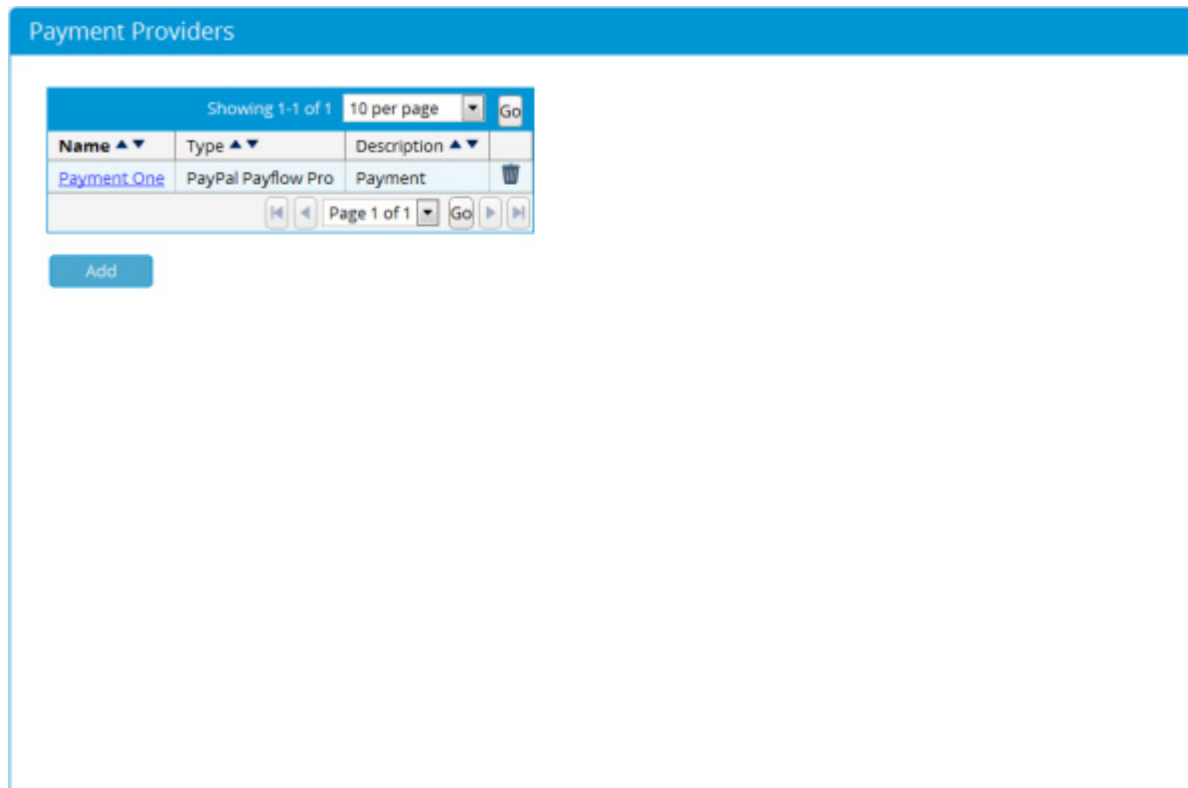
The screenshot shows the 'Add New Payment Provider' form with a blue header. The form is titled 'Account Details' and contains the following fields and sections:

- Account Name:** Text input field.
- Account Description:** Text input field.
- Payment Provider:** Dropdown menu set to 'PayPal Payflow Pro'.
- Operation Mode:** Dropdown menu set to 'Production' with a URL hint '[https://payflowpro.paypal.com]'.
- User:** Text input field.
- Password:** Text input field and **Confirm:** Text input field.
- Merchant Name:** Text input field.
- Partner:** Text input field.
- Available Currencies:** List box containing: Afghani (AFN), Algerian Dinar (DZD), Argentine Peso (ARS), Armenian Dram (AMD), Aruban Guilder (AWG), Australian Dollar (AUD), Azerbaijanian Manat (AZN), Bahamian Dollar (BSD).
- Supported Currencies:** Empty list box.
- Available Cards:** List box containing: Visa, MasterCard, American Express, Diners Club, Discover Card.
- Supported Cards:** Empty list box.

Navigation buttons '<<' and '>>' are located between the 'Available Currencies' and 'Supported Currencies' list boxes, and between the 'Available Cards' and 'Supported Cards' list boxes.

Editing or Deleting a Payment Provider

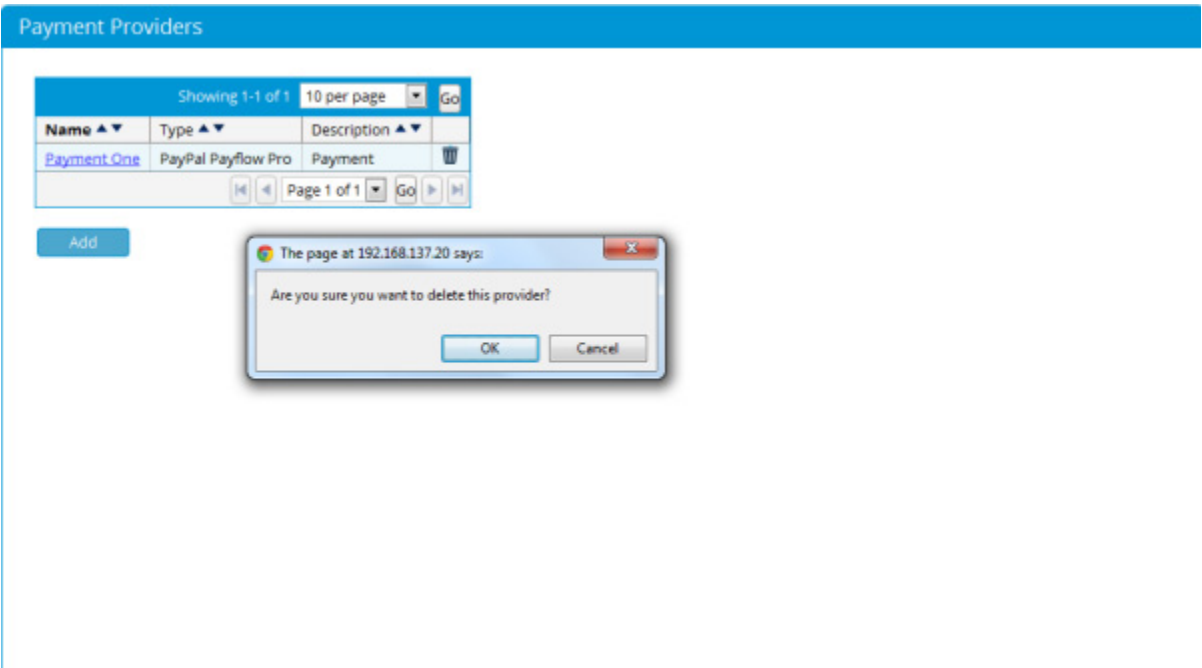
1. From the administration interface, select Guest Portals > Payment Providers as shown below.



2. Click the name of the payment provider you want to edit.
3. Enter the details as follows::
 - Account Name—Enter the name of the payment provider account.
 - Account Description—Enter the description of the payment provider account.
 - Payment Provider—Choose the relevant payment provider from the dropdown menu provided.
 - API Login—Enter the API login for the payment provider account.
 - Transaction Key—Enter the transaction key for the payment provider account.
4. Once completed, click the Save Payment Provider button.

To delete a payment provider :

5. Click on the Bin icon next to the payment provider you wish to delete and click on yes to confirm as shown below.



Payments Reports

Administrators can now run a Payment Report which details all transactions purchased through a Hotspot account.

1. From the Admin UI Interface, go to Reports & Logs->Payments Report, you will be presented with a screen similar to the one below

Payments Report

Payment Method: **Credit Card Billing** Payment Provider: **All**

Portal: **All** Access Plan: **All**

Transaction ID: From: **25** **Nov** **2014**

Username: To: **2** **Dec** **2014**

Name on Card:

Run **Download CSV**

Purchased Guest Accounts Summary

Portal	Number of Accounts	Total
No Records Found		

10 per page **Go**

Transaction ID ▲▼	Name on Card ▲▼	Portal ▲▼	Payment Provider ▲▼	Access Plan	Username ▲▼	Amount ▲▼	Date ▲▼
No Records Found							

2. To run a report on Credit Card Billing select the Credit Card Billing option from the Payment Method field :-
 - Payment Provider - From the drop down menu select a Payment Provider.
 - Portal - From the drop down menu select a Portal.
 - Access Plan - From the drop down menu select an access plan.
 - Transaction ID - From the drop down menu select a Transaction ID.
 - Username - From the drop down menu select a Username.
 - Name on Card - From the drop down menu select a Name on Card.
 - From - From the drop down menu select a From Date.
 - To - From the drop down menu select a To Date.
3. Click Run to display the report on screen, or click Download CSV to download as a file to your desktop.
4. A detailed report will show :-
 - Transaction ID - Users Transaction ID
 - Customer - Users name on card provided.

- Guest Portal - Portal the User accessed.
 - Guest - User account username.
 - Payment Account - Which Payment Provider the User used.
 - Access Plan - Access plan the Used for Guest access.
 - Amount - Amount the User was charged plus tax if required.
 - Date - Date and Time the User user accessed.
5. You can then manually add a transaction for the User.
 - Transaction Type - Select whether you wish to Charge or Refund the User.
 - Amount - Select the amount you wish to Charge or Refund the User.
 - Reason - Add a reason for the Charge or Refund.
 6. Click add to confirm.
 7. Click on the Send Purchase Receipt button to send a receipt of the transaction to the users email address.

Backup and Restore

You should backup the FortiConnect on a regular basis so that in the event of a hardware failure you do not lose critical data. The FortiConnect backup process backs up the system setup, account database, and all audit records, enabling you to recover everything you need in the event of a failure. You can either create a “point-in-time” snapshot, or schedule system backups to be automatically saved to the FortiConnect or a remote FTP server.

This chapter includes the following sections:

- Configuring Backup
- Restoring Backups

Configuring Backup

This section describes the following

- Setting Backup Settings
- Taking Snapshots
- Scheduling Backups

Setting Backup Settings

1. From the administration home page, select **Server > Backup/Restore** as shown below.

Backup/Restore

Backup Settings | Backup Schedule | Restore a Backup File | Manage Backup Files

Backup Type: **FTP and local backup**

Server:

Port:

Passive Mode: ☒

Directory:

Username:

Password: Confirm:

Max number of server backups:
Leave blank for unlimited backup files

Save **Cancel** **Test Remote Backup**

Snapshot

Download: **Snapshot**

2. To perform the backup to a remote FTP server, click the Backup Settings tab:
 - Enter the Remote Server Address for the FTP server.
 - Enter the TCP Port to be used (usually port 21).
 - Enter the Directory to store the backup.
 - Enter a Username and Password (confirming the password) that allows access to the FTP server.
 - Selecting the Mode is Passive box activates passive for the FTP Mode. Leaving it unchecked keeps this inactive.
3. Click the Save Settings button to save the backup settings.

Taking Snapshots

You can save a point-in-time snapshot to allow you to download a backup of the FortiConnect at an exact moment.

1. From the administration home page, select Server > Backup/Restore and select the Backup Settings tab.
2. To save a snapshot backup, click the Snapshot button at the bottom of the form.

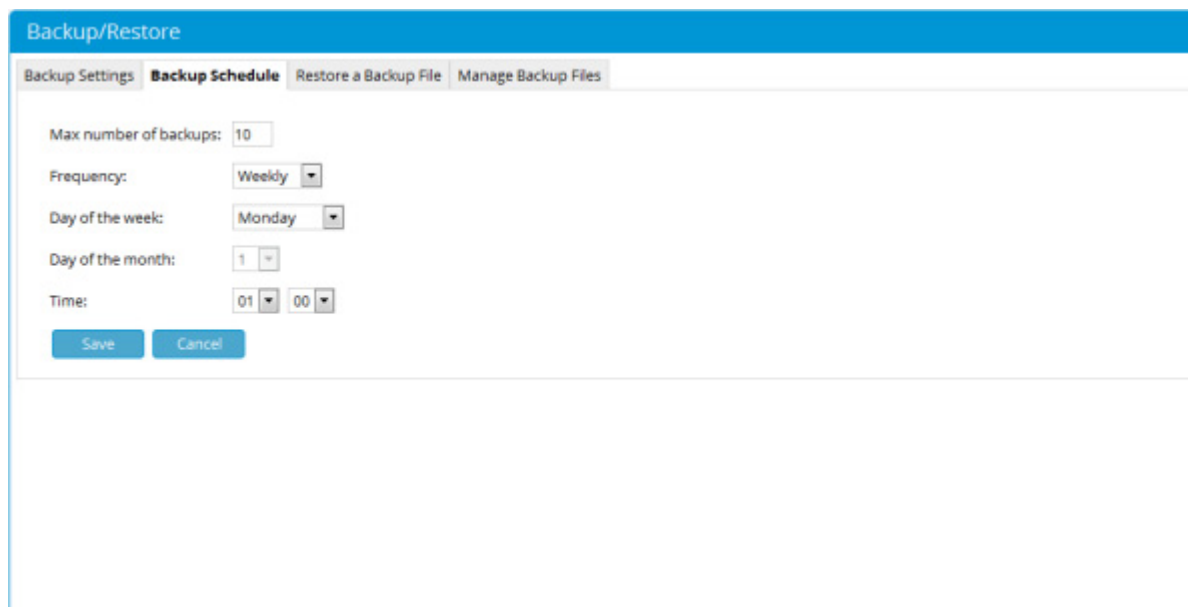
3. You are prompted by your web browser to save the backup file to disk.

Note: You will receive a warning in your 'Audit Log' messages if there is insufficient disk space to complete the operation. The default disk space requirement is 40% of the database.

Scheduling Backups

You can schedule backups to occur every day, week, or month at 1:00 AM. Scheduled backups are stored in either the /guest/backup directory of the FortiConnect or on a remote FTP server.

1. From the administration home page, select Server > Backup/Restore and select the Backup Schedule tab as shown below.



The screenshot shows the 'Backup/Restore' configuration page with the 'Backup Schedule' tab selected. The page has a blue header bar with the title 'Backup/Restore'. Below the header, there are four tabs: 'Backup Settings', 'Backup Schedule' (which is active), 'Restore a Backup File', and 'Manage Backup Files'. The 'Backup Schedule' tab contains the following settings:

- Max number of backups: 10
- Frequency: Weekly (dropdown menu)
- Day of the week: Monday (dropdown menu)
- Day of the month: 1 (dropdown menu)
- Time: 01:00 (time picker)

At the bottom of the settings area, there are two buttons: 'Save' and 'Cancel'.

2. To perform local backups:
 - Enter the Maximum number of backups that you want to save. The FortiConnect removes old backups that exceed this amount by discarding the oldest backup when new ones are created. Note - If you do not want to limit the number of files, you can specify a number less than 1, for example, 0 or -1.
 - Specify how often you want the FortiConnect to perform backups in the Frequency dropdown menu. You can specify Daily, Weekly, or Monthly. If you select Weekly you must also specify which day of the week. If you select Monthly, you must specify which day of the month.

Note: Fortinet recommends specifying a date between the 1st and 28th day of the month to ensure that you automatically back up your system every month of the year.

3. Click the Save Settings button to save settings.

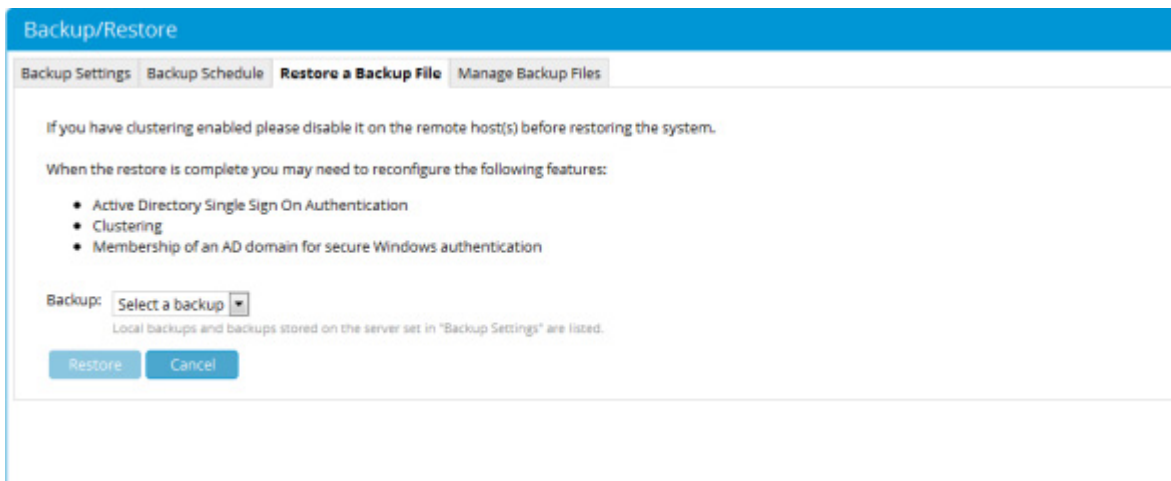
Note: You will receive a warning in your 'Audit Log' messages if there is insufficient disk space to complete the operation. The default disk space requirement is 40% of the database.

Restoring Backups

You can restore a backup to the FortiConnect from the administration interface.

Note: You can only restore a backup to the same version of FortiConnect software with which the backup was performed. If you need to determine which version was used to perform the backup, open the backup archive file directory and view the version.html file in the backup archive.

1. From the administration home page, select Server > Backup/Restore and click the Restore a Backup File tab as shown below.



Backup/Restore

Backup Settings Backup Schedule **Restore a Backup File** Manage Backup Files

If you have clustering enabled please disable it on the remote host(s) before restoring the system.

When the restore is complete you may need to reconfigure the following features:

- Active Directory Single Sign On Authentication
- Clustering
- Membership of an AD domain for secure Windows authentication

Backup: Select a backup ▼

Local backups and backups stored on the server set in "Backup Settings" are listed.

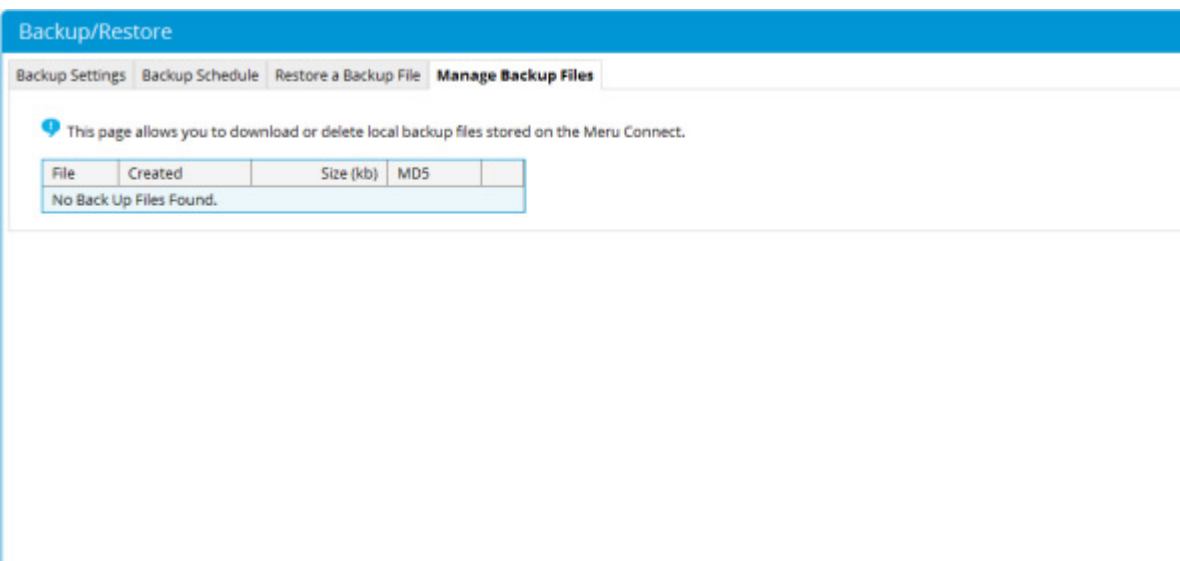
Restore Cancel

2. From the Backup dropdown menu select the backup archive you want to restore.
3. Click the Restore button.
4. The backup is uploaded to the FortiConnect and the data is restored. Once the data has been restored, the server will reboot so that the database is correctly loaded.

Manage Backups

You can manage all the backups you have performed using FortiConnect.

1. From the FortiConnect Administration interface select Server --> Backup/Restore and click on the Manage Backup Files tab as shown below.



2. From here you can click on the Download Icon to save a file locally, or click on the Bin icon to delete the file.

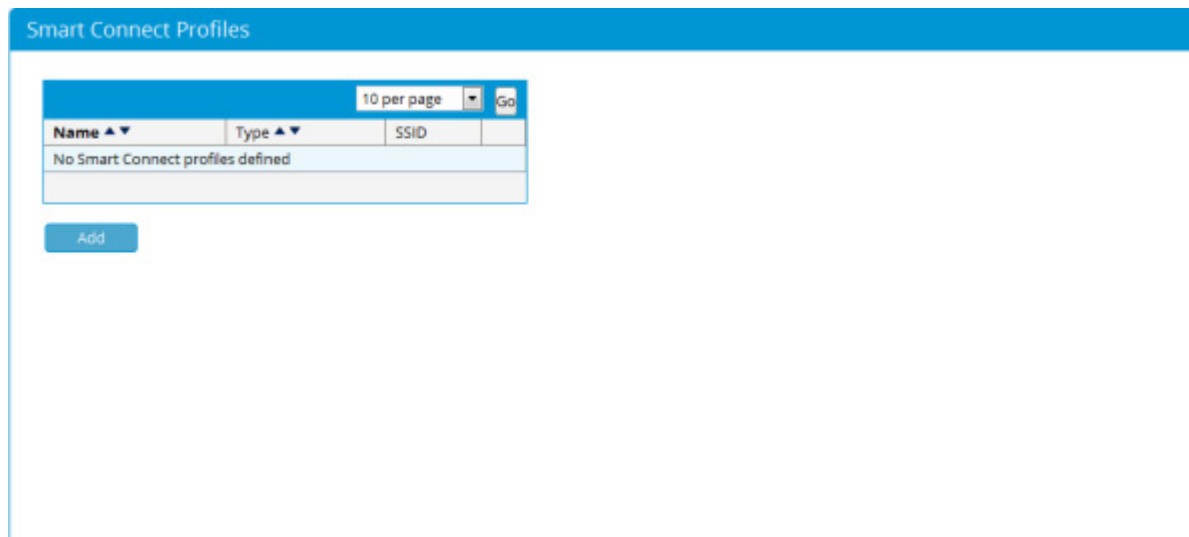
Smart Connect

This section details how to use the setup wizard within FortiConnect to enable Smart Connect.

Smart Connect has the ability to configure wireless profiles and ensure that users are provisioned and connected to the secure network across a range of laptops, phones, and tablets.

Adding a Smart Connect Profile

To add a Network Profile for Smart Connect go to the Smart Connect --> Smart Connect Profiles section on the FortiConnect administration database as shown below.

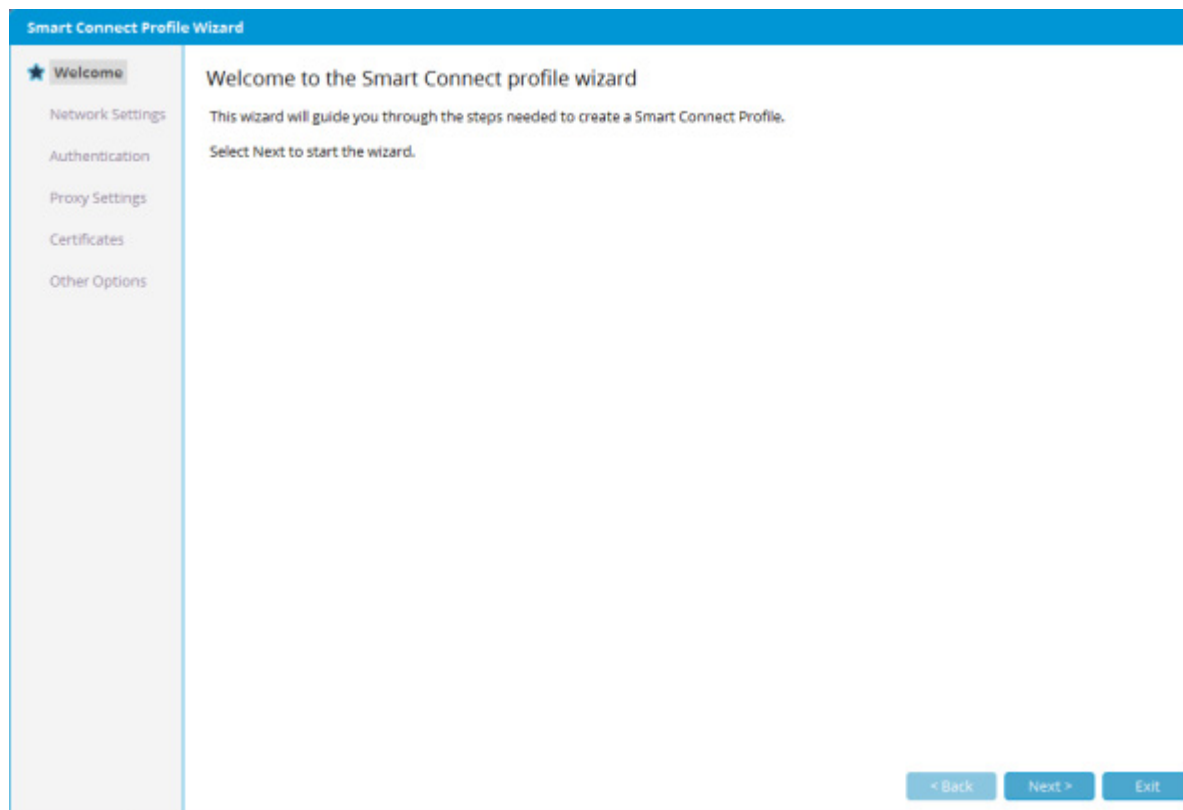


Name ▲▼	Type ▲▼	SSID
No Smart Connect profiles defined		

Add

Click on the add button to add a new profile and to start the setup wizard.

Adding a Smart Connect Profile



Click on Next to enter the Network Settings as shown below.

Smart Connect Profile Wizard

✓ Welcome

★ **Network Settings**

Authentication

Proxy Settings

Certificates

Other Options

Network Settings

Please provide a name and type for the network.

Network Name:

Network Type: ☐ wired ☒ wireless

SSID:

SSID is Broadcast: ☒

Remove SSIDs

Please enter the SSIDs that you would like to remove from the client.
It is advisable to remove the SSIDs for any open networks that you don't want the client to automatically connect to.

< Back Next > Exit

1. Network Name - Enter a name for your network
2. Network Type - Select a network type.
 - Wired - If it is a wired network then no further information is required, click on Next to continue.
 - Wireless - If it is a wireless network then :-
 - ⑧ Enter the SSID name
 - ⑧ Place a check in the checkbox if the SSID is broadcast.
 - ⑧ You can also enter the names of any SSID's you wish to remove.
3. Click on Next to continue.

Now enter any Authentication settings as shown below.

Adding a Smart Connect Profile

The screenshot shows the 'Smart Connect Profile Wizard' with the 'Authentication' step selected in the left sidebar. The main area is titled 'Authentication' and contains the following fields and options:

- Please provide the authentication details for the network.**
- Authentication:** A dropdown menu set to 'WPA/WPA2 Enterprise'. Below it, a note states 'Windows systems will use WPA2'.
- EAP Type:** Four dropdown menus for different operating systems:
 - Windows: PEAP/MSCHAPv2
 - Apple iOS / OS X: PEAP/MSCHAPv2 and PEAP/GTC
 - Android: PEAP/GTC
 - Linux: PEAP/GTC
- PEAP/MSCHAPv2 and PEAP/GTC** (Section Header):
 - Include Credentials:** Two radio buttons: 'Include username/password in profile sent to user' (selected) and 'Don't include username/password in profile sent to user'.
 - Authenticate with:** Four radio buttons: 'realm/username', 'realm/Username', 'username@realm', and 'username' (selected).
 - Realm:** A text input field.
 - Detect and override username format and realm when authenticating against Active Directory:** A checked checkbox.

At the bottom right, there are three buttons: '< Back', 'Next >', and 'Exit'.

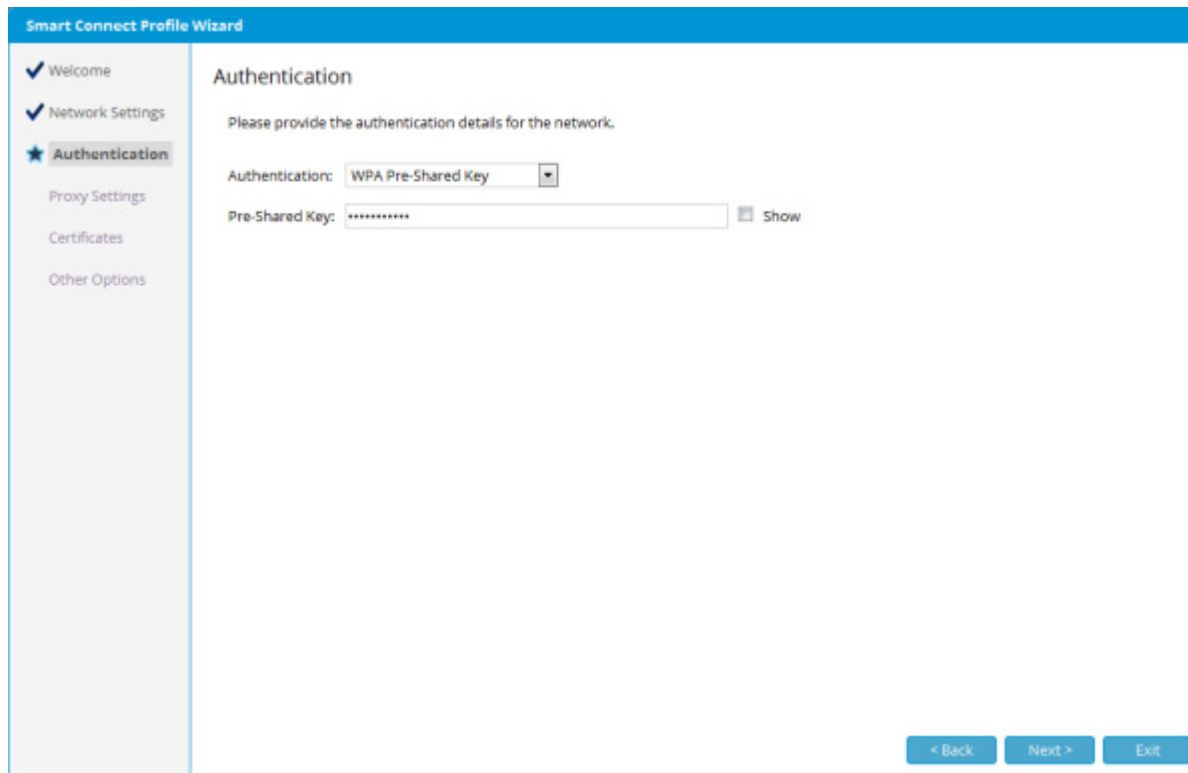
If in the Network Settings page you selected a wireless network type, then from the drop down menu select your Authentication method.

There are two main types of Authentication to choose from, Enterprise and Pre-Shared Key, depending on the option you choose you will be required to enter different credentials.

If selecting an Enterprise option then :-

4. EAP Type - Using the drop down menu select an EAP Type for Authentication
5. Include Credentials - Using the check boxes provided decide whether you want to 'Include' or 'Don't include' username/password in profile sent to the user.
6. Authenticate with - Check one of the options to use that particular username format, and then define the realm.
7. Detect and override username format when authenticating against Active Directory
8. EAP/TLS - If your EAP Type was EAP-TLS then use the drop down menu to select where to Generate Certificates from. Details on how to do this are at the bottom of the Smart Connect Section under SCEP Server and User Certificate Authority.

If selecting a Pre-Shared Key option then your options differ as shown below.



The image shows the 'Smart Connect Profile Wizard' window. On the left is a sidebar with a list of steps: 'Welcome' (checked), 'Network Settings' (checked), 'Authentication' (selected with a star icon), 'Proxy Settings', 'Certificates', and 'Other Options'. The main area is titled 'Authentication' and contains the text 'Please provide the authentication details for the network.' Below this, there is a dropdown menu for 'Authentication' currently set to 'WPA Pre-Shared Key'. Underneath is a text field for the 'Pre-Shared Key' containing several asterisks, followed by a 'Show' button with an eye icon. At the bottom right of the window are three buttons: '< Back', 'Next >', and 'Exit'.

9. Pre-Shared Key - Enter the Pre-Shared Key in the field provided and click the show box if you wish to display this.

If in the Network Settings page you selected a wired network type, then your options will differ from those above, the only authentication you can choose is 802.1X as shown below.

Adding a Smart Connect Profile

The screenshot shows the 'Smart Connect Profile Wizard' with the 'Authentication' step selected in the left sidebar. The main area is titled 'Authentication' and contains the following fields and options:

- Please provide the authentication details for the network.**
- Authentication:** A dropdown menu showing 'IEEE 802.1x'.
- EAP Type:** A table with four rows: Windows, Apple iOS / OS X, Android, and Linux. Each row has a corresponding dropdown menu for the EAP Type.

Platform	EAP Type
Windows	PEAP/MSCHAPv2
Apple iOS / OS X	PEAP/MSCHAPv2 and PEAP/GTC
Android	PEAP/GTC
Linux	PEAP/GTC
- PEAP/MSCHAPv2 and PEAP/GTC** (Section Header)
 - Include Credentials:** Two radio buttons: 'Include username/password in profile sent to user' (selected) and 'Don't include username/password in profile sent to user'.
 - Authenticate with:** Four radio buttons: 'realm \username', 'realm/username', 'username@realm', and 'username' (selected).
 - Realm:** A text input field.
 - Detect and override username format and realm when authenticating against Active Directory:** A checked checkbox.

At the bottom right, there are three buttons: '< Back', 'Next >', and 'Exit'.

10. EAP Type - Using the drop down menu select an EAP Type for Authentication

11. Include Credentials - Using the check boxes provided decide whether you want to 'Include' or 'Don't include' username/password in profile sent to the user.

12. Authenticate with - Check one of the options to use that particular username format, and then define the realm.

13. Detect and override username format when authenticating against Active Directory

14. EAP/TLS - If your EAP Type was EAP-TLS then use the drop down menu to select where to Generate Certificates from. Details on how to do this are at the bottom of the Smart Connect Section under SCEP Server and User Certificate Authority.

Once completed click on Next to continue onto configuring the clients Proxy Server Settings as shown on the screen below.

15. Using the drop down menus select from the following :-

- Apple OS X proxy Mode - From the drop down menu, select whether Proxy Server Settings should be Disabled or set to Auto Discovery.
- Windows Proxy Mode - From the drop down menu, select whether Proxy Server Settings should be Disabled or set to Auto Discovery.
- Android Proxy Mode - From the drop down menu, select whether Proxy Server Settings should be Disabled or set to Manual Settings. For info on manual settings see below.
- Linux Proxy Mode - From the drop down menu, select whether Proxy Server Settings should be Disabled or set to Auto Discovery.
- Apple IOS Proxy Mode - From the drop down menu, select whether Proxy Server Settings should be Auto Discovery, Pac URL, Disabled or set to Manual Settings. For info on manual settings and PAC URL see below.

To enter the Manual Settings for your proxy server settings :-

- Server - Enter your servers hostname or IP Address
- Port - Enter the appropriate port number

Adding a Smart Connect Profile

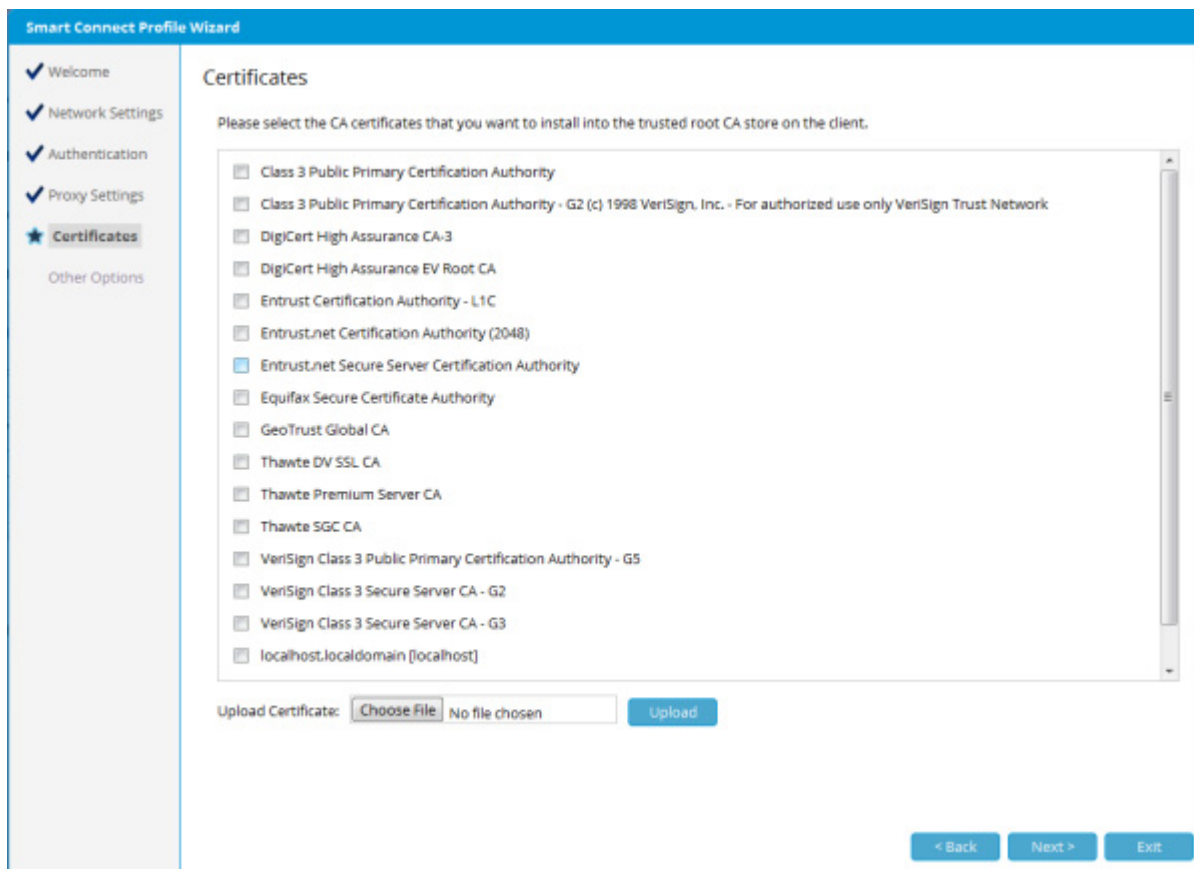
- **Authentication** - From the drop down menu select whether no authentication is needed or whether a login is required then follow the next steps
- **Username** - Enter the username for authentication
- **Password** - Enter and confirm the password
- **Username Format** - Select a method of username format
- **Realm** - Enter the Realm if required.

To enter PAC URL settings for your proxy server :-

- **ProxyPACURLString Optional** - The URL of the PAC file that defines the proxy configuration.
- **ProxyPACFallbackAllowed Boolean Optional** -If false, prevents the device from connecting directly to the destination if the PAC file is unreachable. Default is true.

Once completed click on Next to continue to the Certificates screen as shown below.

Note: This screen will only display if Pre-Shared Key hasn't been selected as an Authentication method. If Pre-Shared Key has been selected then skip straight to the User Assignment section.



The screenshot shows the 'Smart Connect Profile Wizard' interface, specifically the 'Certificates' step. On the left, a sidebar lists the wizard steps: Welcome, Network Settings, Authentication, Proxy Settings, and Certificates (which is highlighted with a star). Below the sidebar, the main content area is titled 'Certificates' and contains the instruction: 'Please select the CA certificates that you want to install into the trusted root CA store on the client.' Below this instruction is a list of 15 CA certificates, each with a checkbox. The 'Entrust.net Secure Server Certification Authority' is selected. At the bottom of the list, there is an 'Upload Certificate:' section with a 'Choose File' button, a text field showing 'No file chosen', and an 'Upload' button. At the very bottom of the wizard, there are three buttons: '< Back', 'Next >', and 'Exit'.

Smart Connect Profile Wizard

✓ Welcome
✓ Network Settings
✓ Authentication
✓ Proxy Settings
★ Certificates
Other Options

Certificates

Please select the CA certificates that you want to install into the trusted root CA store on the client.

- ☐ Class 3 Public Primary Certification Authority
- ☐ Class 3 Public Primary Certification Authority - G2 (c) 1998 VeriSign, Inc. - For authorized use only VeriSign Trust Network
- ☐ DigiCert High Assurance CA-3
- ☐ DigiCert High Assurance EV Root CA
- ☐ Entrust Certification Authority - L1C
- ☐ Entrust.net Certification Authority (2048)
- ☒ Entrust.net Secure Server Certification Authority
- ☐ Equifax Secure Certificate Authority
- ☐ GeoTrust Global CA
- ☐ Thawte DV SSL CA
- ☐ Thawte Premium Server CA
- ☐ Thawte SGC CA
- ☐ VeriSign Class 3 Public Primary Certification Authority - G5
- ☐ VeriSign Class 3 Secure Server CA - G2
- ☐ VeriSign Class 3 Secure Server CA - G3
- ☐ localhost.localdomain [localhost]

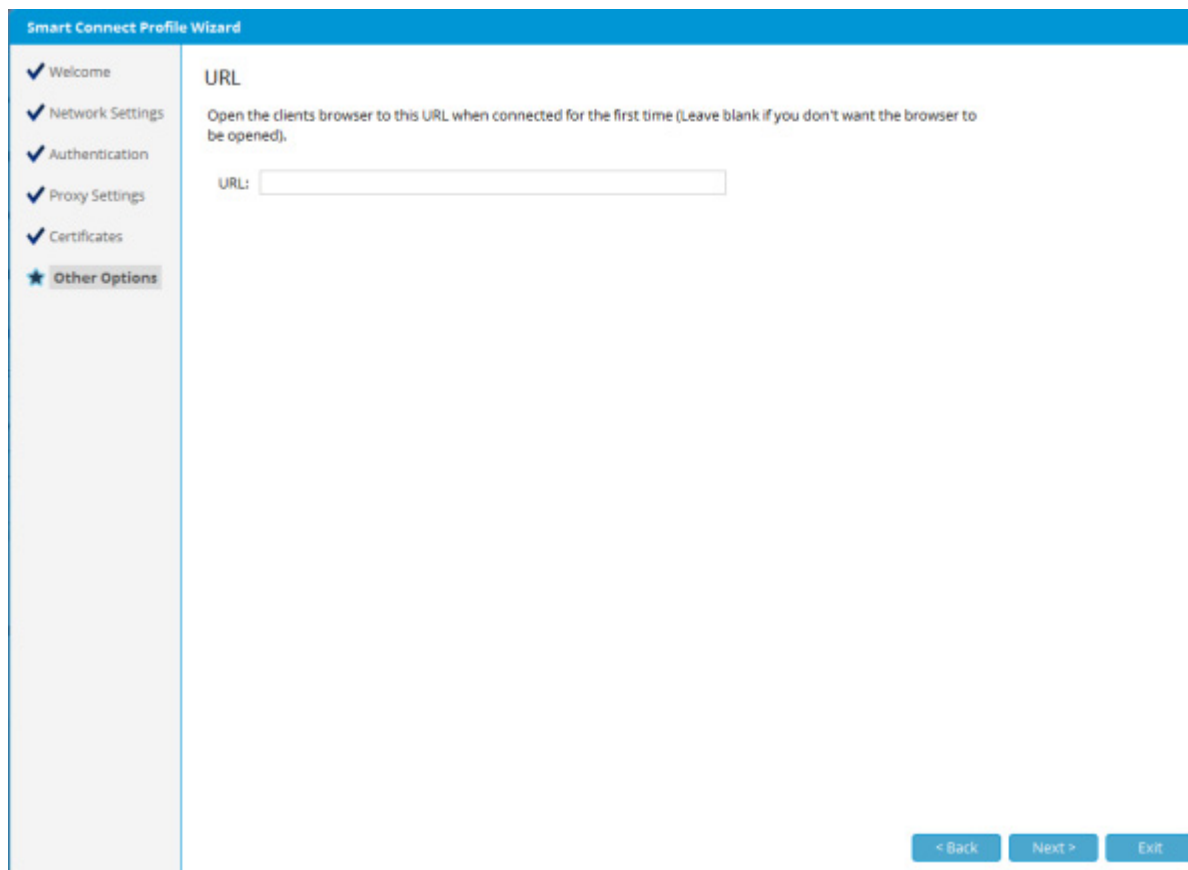
Upload Certificate: No file chosen

< Back Next > Exit

- Upload Certificate - Click on the Browse button and upload any certificates you wish to install.
- Or, using the check boxes, select any of the pre-installed certificates available on the Identity Manager.
- Click on Next to continue.

Next you will be taken to the Other Options screen as shown below.

Note: The certificate for the FortiConnect is denoted by [localhost]

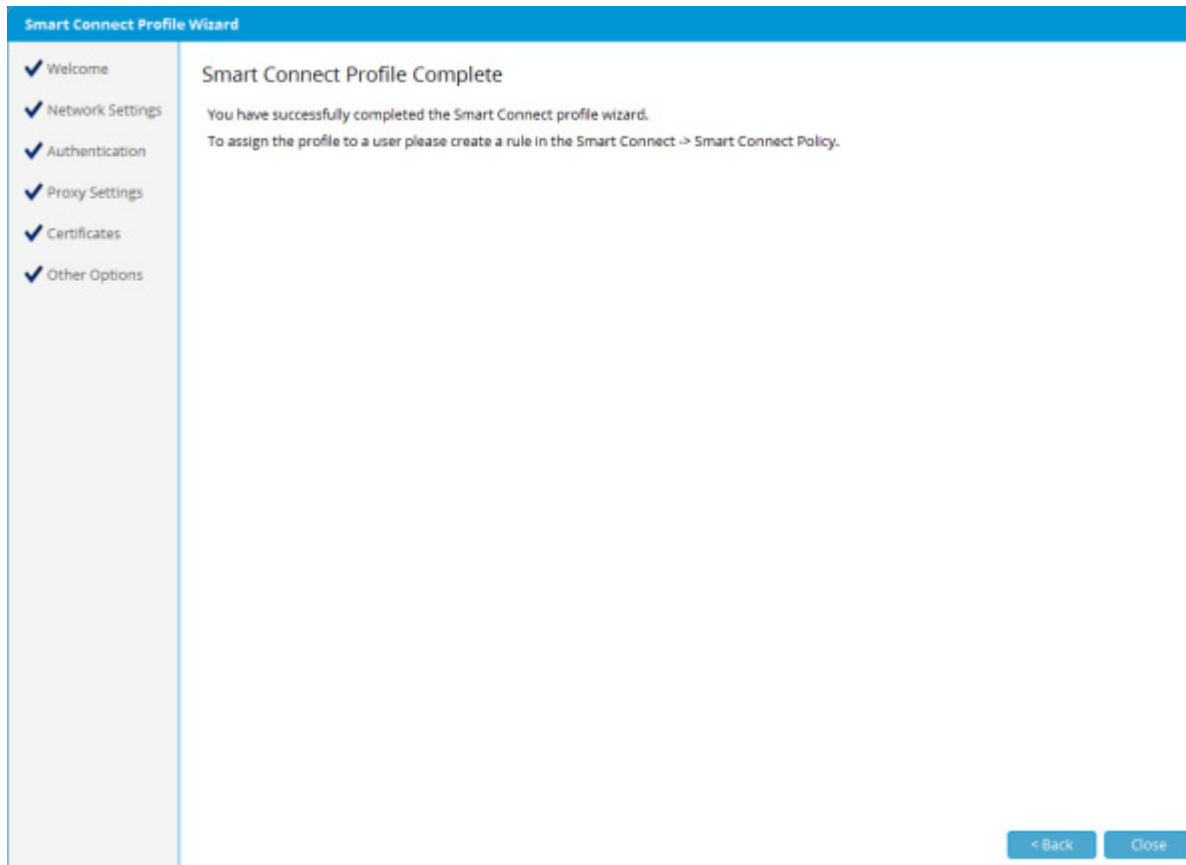


The screenshot shows the 'Smart Connect Profile Wizard' interface. On the left is a vertical sidebar with a list of steps: 'Welcome', 'Network Settings', 'Authentication', 'Proxy Settings', 'Certificates', and 'Other Options'. The first five steps are marked with a checkmark, and 'Other Options' is marked with a star. The main area of the wizard is titled 'URL' and contains the instruction: 'Open the clients browser to this URL when connected for the first time (Leave blank if you don't want the browser to be opened)'. Below this instruction is a text input field labeled 'URL:'. At the bottom right of the wizard, there are three buttons: '< Back', 'Next >', and 'Exit'.

- URL - Enter the URL you wish to direct the browser to once connected, after Smart Connect has run.
- Click Next to continue.

You have now successfully setup a Smart Connect Profile.

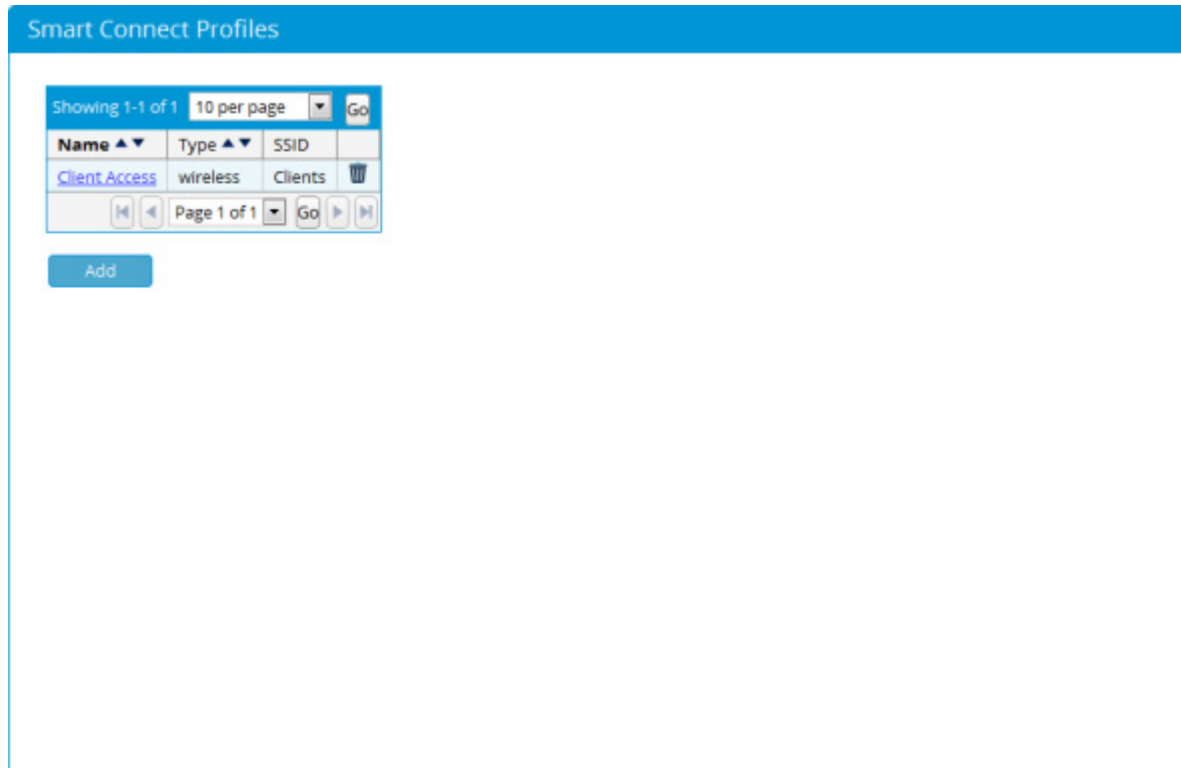
Note: This does not apply to Apple Devices configured using an Apple configuration profile.



Click Close to complete.

Editing a Smart Connect Profile

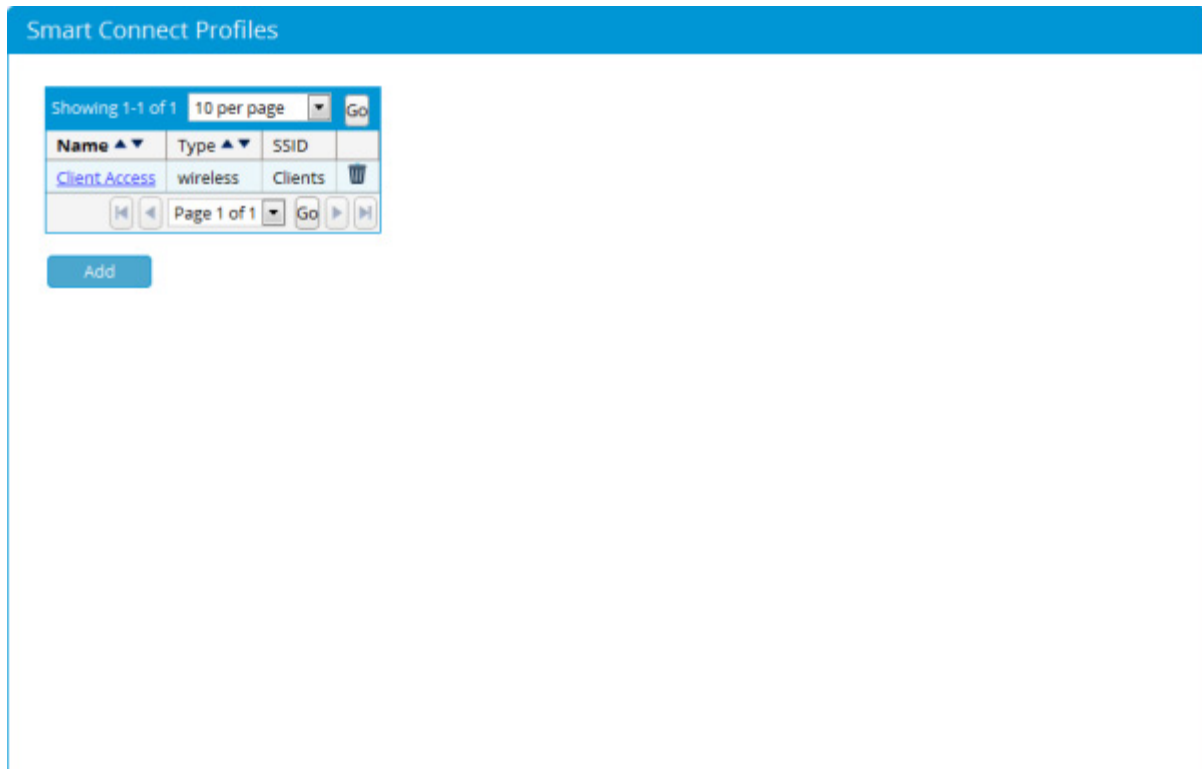
To Edit a Network Profile go to Smart Connect --> Smart Connect Profiles as shown below



Click on the link of the Smart Connect Profile you wish to configure underneath the Name Column. This will open up the Smart Connect Profile setup wizard, follow the steps as detailed in the Adding a Smart Connect Profile section to complete your changes.

Deleting a Smart Connect Profile

To delete a Smart Connect Profile, go to Smart Connect --> Smart Connect Profiles from the Administration interface as shown below.



Click on the Bin Icon to the right of the Smart Connect Profile you wish to delete, click on yes to confirm deletion.

Smart Connect Policy

A Smart Connect Policy defines which Smart Connect Profile is applied to each user. Once a user is authenticated and authorized FortiConnect applies Smart Connect Policy rules on that user to find the appropriate Smart Connect Profile for that user to connect to the secure network.

All policies are checked in a specific order, defined by the Administrator, if a policy is matched then the remaining policies are ignored. If no policy gets matched then the Default Smart Connect Policy is applied.



Add a Smart Connect Policy

1. From the FortiConnect Administration interface go to Smart Connect --> Smart Connect Policy as shown below.

Smart Connect Policy

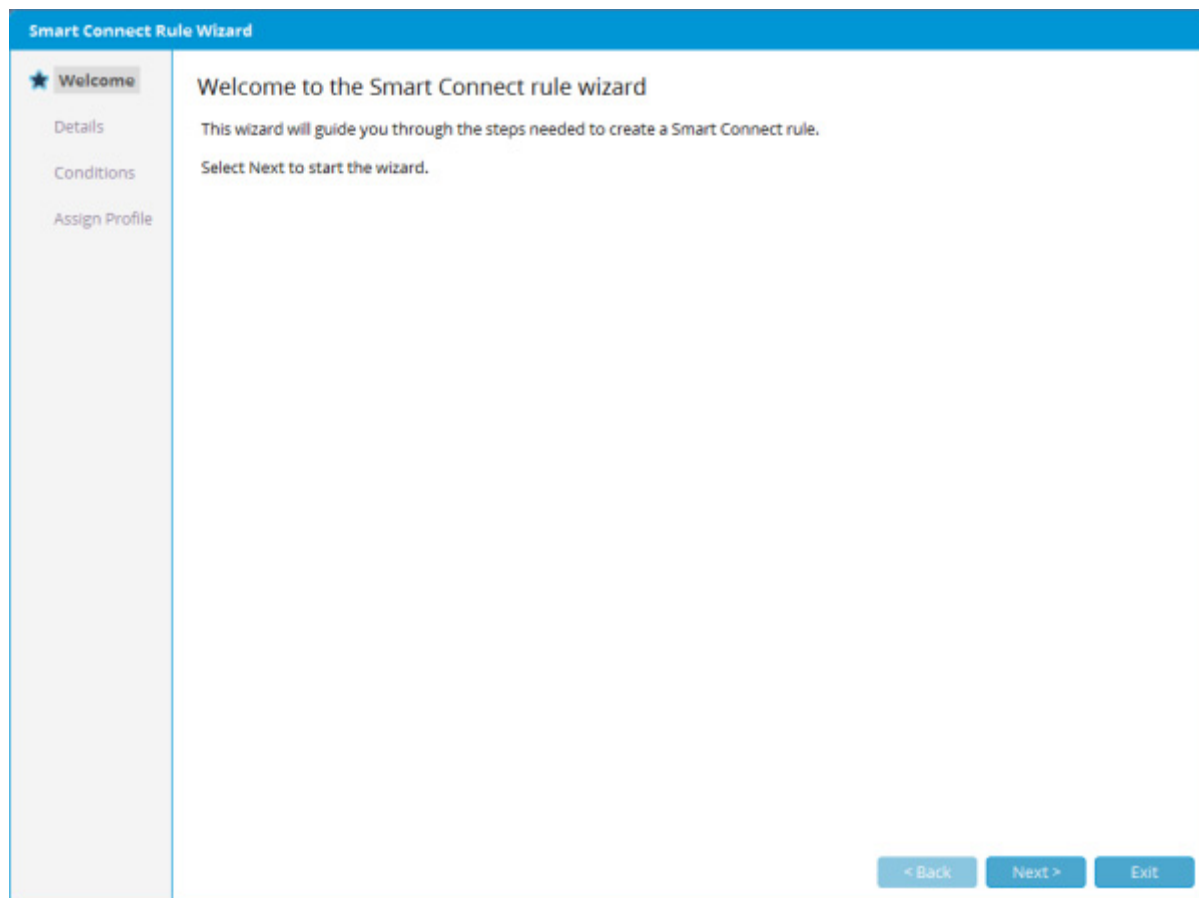
The Smart Connect policy defines which Smart Connect profiles are applied to each user.

Each Smart Connect policy is checked in the following order. First matched policy is applied and no other policies are checked.

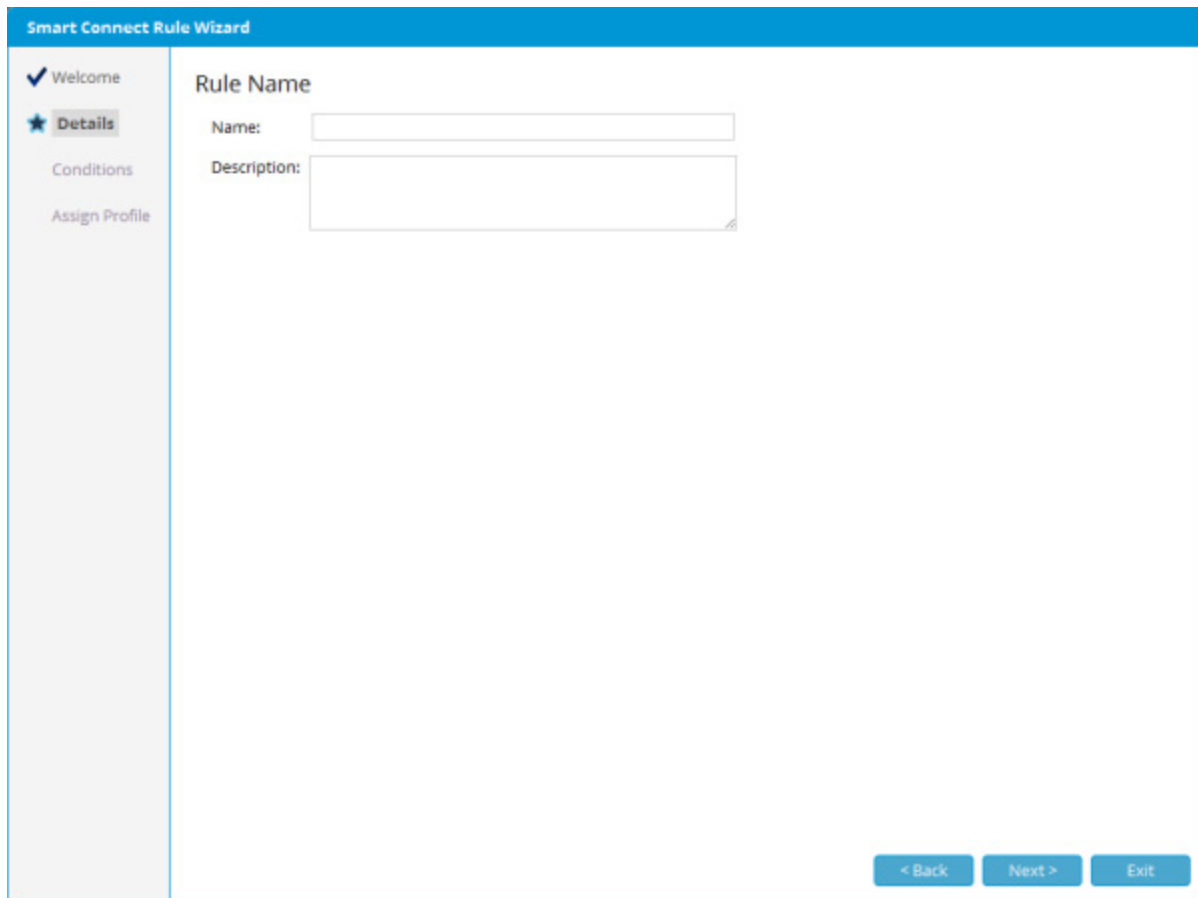
Order	Name	Rule	Wired Profiles	Wireless Profiles	Enabled	Action
1	Default	default rule	No Smart Connect			

Save OrderAdd

2. Click on the Add button to bring up the Smart Connect Rule Wizard.

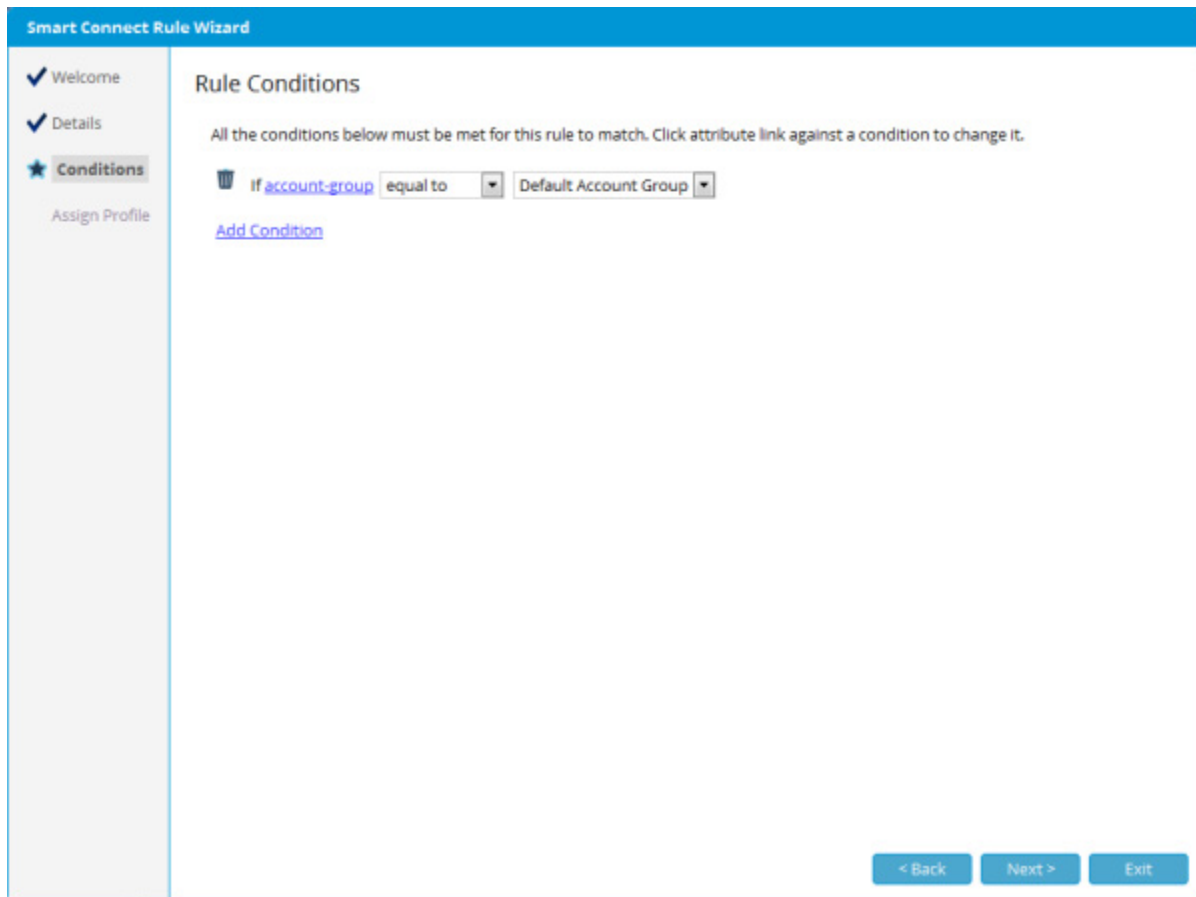


3. Click on Next to start the Wizard.



The image shows a screenshot of the 'Smart Connect Rule Wizard' interface. The title bar at the top is blue and contains the text 'Smart Connect Rule Wizard'. On the left side, there is a vertical sidebar with four items: 'Welcome' (with a checkmark icon), 'Details' (with a star icon and highlighted with a grey background), 'Conditions', and 'Assign Profile'. The main area of the wizard is titled 'Rule Name' and contains two input fields: 'Name:' with a single-line text box, and 'Description:' with a larger multi-line text box. At the bottom right of the main area, there are three buttons: '< Back', 'Next >', and 'Exit'.

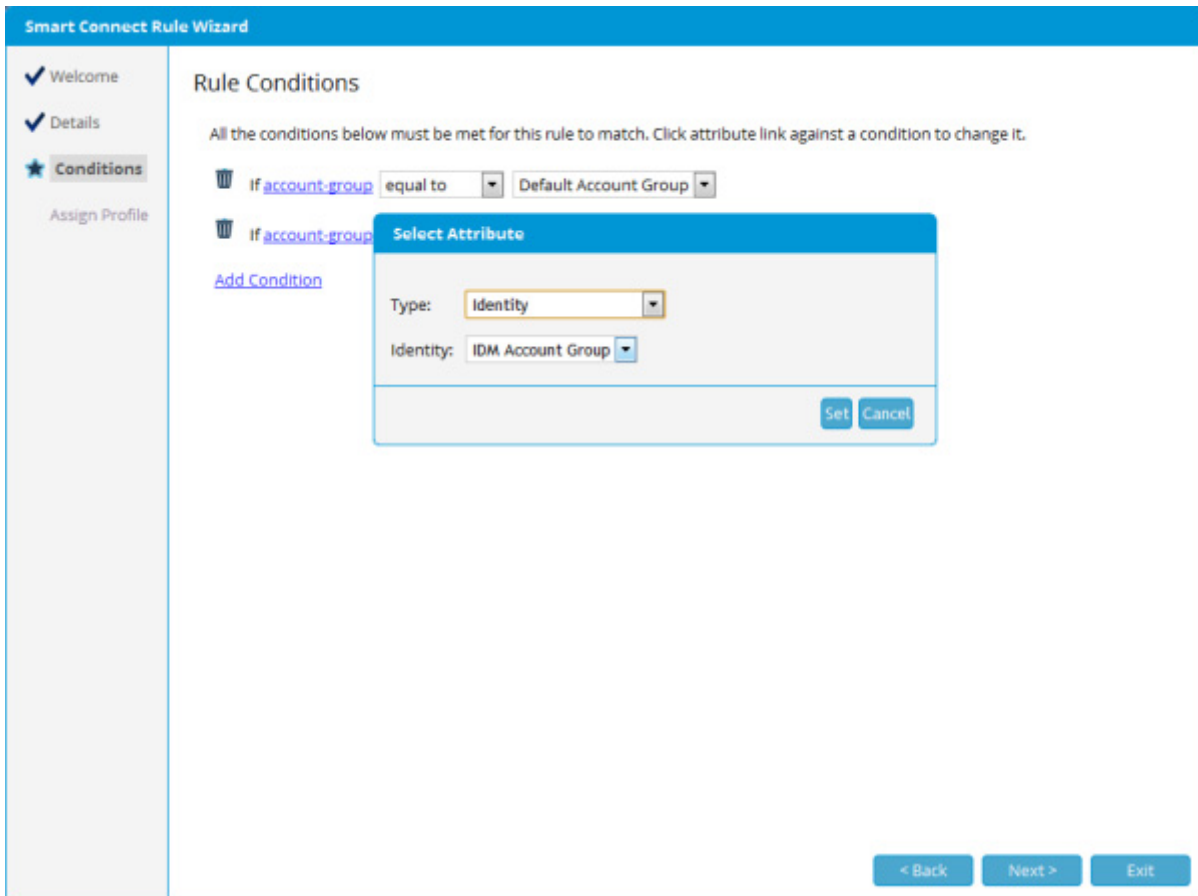
4. Enter a name for your Rule and a Description in the fields provided then click on Next.



The image shows the 'Smart Connect Rule Wizard' interface, specifically the 'Rule Conditions' step. On the left sidebar, the 'Conditions' step is highlighted with a star icon, and 'Assign Profile' is listed below it. The main area is titled 'Rule Conditions' and contains the instruction: 'All the conditions below must be met for this rule to match. Click attribute link against a condition to change it.' Below this, there is a single condition: 'If [account-group](#) equal to '. A trash icon is to the left of the condition. Below the condition is a blue link labeled 'Add Condition'. At the bottom right, there are three buttons: '< Back', 'Next >', and 'Exit'.

5. You can now add Conditions to your policy by adding attributes, click on the attribute link to add as shown below. To add more conditions click on the Add Condition link.

Note: By Default, all users are assigned to the Default Account Group



The screenshot shows the 'Smart Connect Rule Wizard' interface. On the left, a sidebar contains a navigation menu with 'Welcome', 'Details', and 'Conditions' (the active tab, marked with a star). Below the menu is the text 'Assign Profile'. The main area is titled 'Rule Conditions' and contains the instruction: 'All the conditions below must be met for this rule to match. Click attribute link against a condition to change it.' There are two conditions listed, each with a trash icon and a blue underlined attribute link 'account-group'. The first condition is 'If account-group equal to Default Account Group'. The second condition is 'If account-group'. A modal window titled 'Select Attribute' is open over the second condition. It has two dropdown menus: 'Type' set to 'Identity' and 'Identity' set to 'IDM Account Group'. At the bottom of the modal are 'Set' and 'Cancel' buttons. At the bottom of the main window are '< Back', 'Next >', and 'Exit' buttons.

Smart Connect Rule Wizard

✓ Welcome
✓ Details
★ **Conditions**
Assign Profile

Rule Conditions

All the conditions below must be met for this rule to match. Click attribute link against a condition to change it.

- ✖ If [account-group](#) equal to Default Account Group
- ✖ If [account-group](#)

[Add Condition](#)

Select Attribute

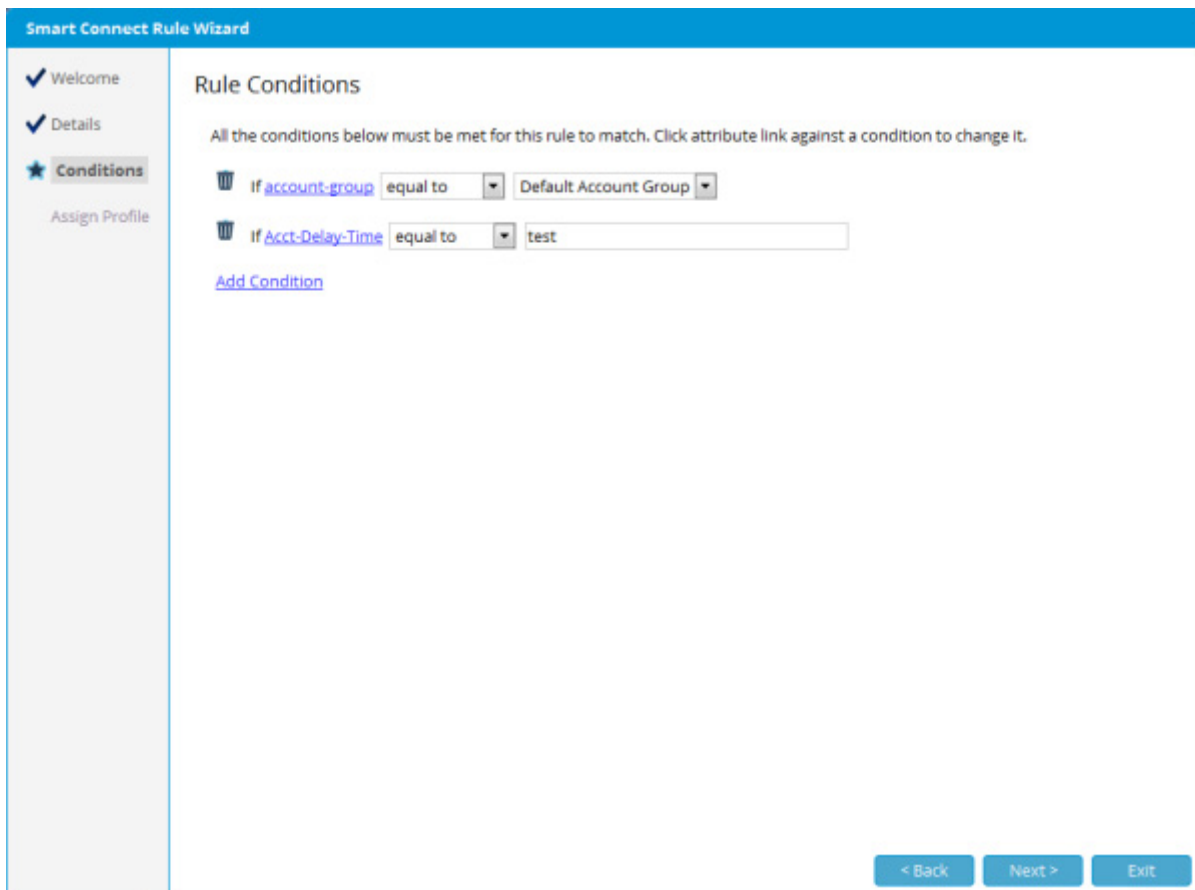
Type: Identity

Identity: IDM Account Group

Set Cancel

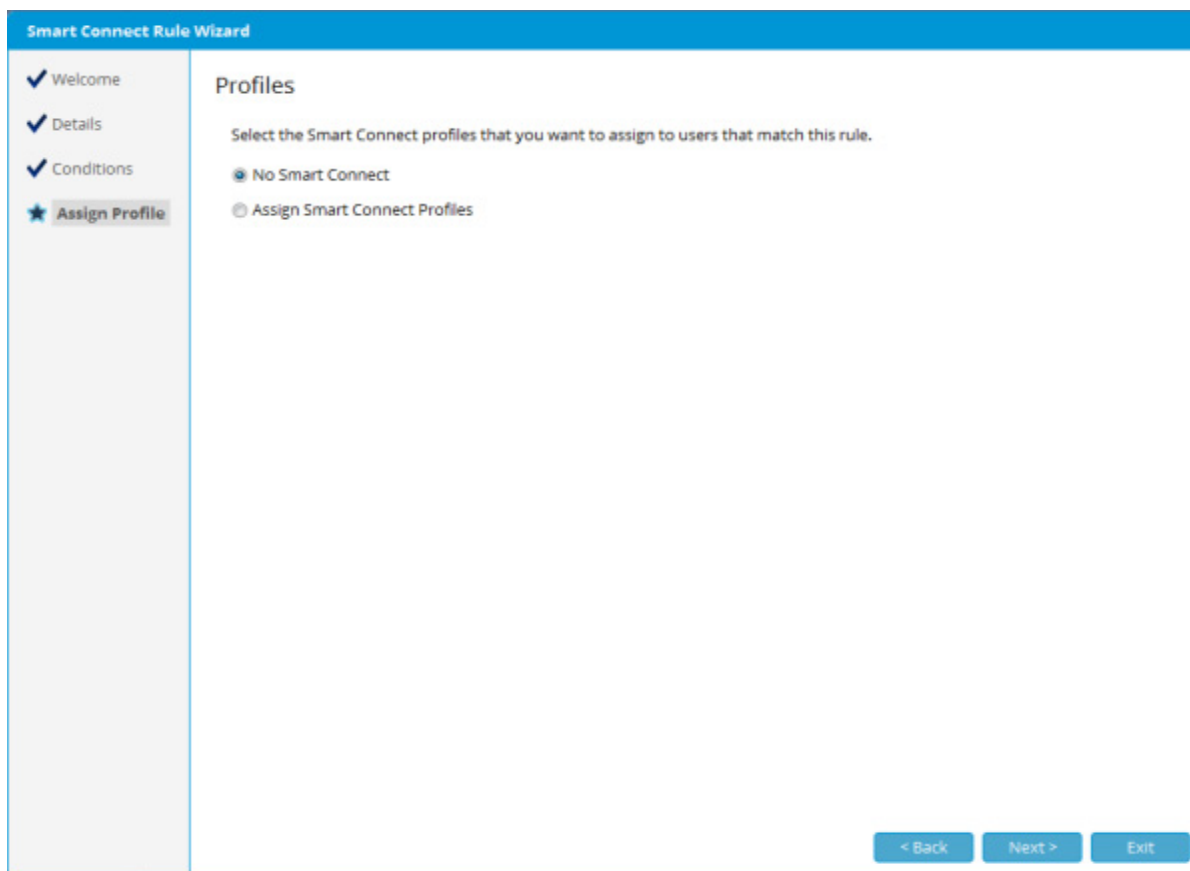
< Back Next > Exit

6. Select the appropriate Attribute from the drop down menu and click on Set.



The image shows the 'Smart Connect Rule Wizard' interface, specifically the 'Rule Conditions' step. On the left, a sidebar contains a navigation menu with 'Welcome', 'Details', 'Conditions' (highlighted with a star), and 'Assign Profile'. The main area is titled 'Rule Conditions' and includes a sub-header: 'All the conditions below must be met for this rule to match. Click attribute link against a condition to change it.' There are two conditions listed, each with a trash icon on the left. The first condition is 'If [account-group](#) equal to [dropdown] Default Account Group [dropdown]'. The second condition is 'If [Acct-Delay-Time](#) equal to [dropdown] test'. Below the conditions is a link that says 'Add Condition'. At the bottom right, there are three buttons: '< Back', 'Next >', and 'Exit'.

7. Complete the Condition by using the drop down menu and the fields provided.
8. Click Next once you have finished entering your conditions.



The image shows the 'Smart Connect Rule Wizard' interface, specifically the 'Profiles' step. On the left, a sidebar lists the steps: 'Welcome', 'Details', 'Conditions', and 'Assign Profile' (which is highlighted with a star). The main area is titled 'Profiles' and contains the instruction: 'Select the Smart Connect profiles that you want to assign to users that match this rule.' Below this, there are two radio button options: 'No Smart Connect' (which is selected) and 'Assign Smart Connect Profiles'. At the bottom right, there are three buttons: '< Back', 'Next >', and 'Exit'.

9. Select the Smart Connect Profiles that you want to assign to users that match the rule you have created.

- No Smart Connect - Select if the profile should not be assigned a Smart Connect Profile.
- Assign Smart Connect - Select to assign a Smart Connect profile.

Wired - select which Smart Connect profile to assign for Wired profiles.

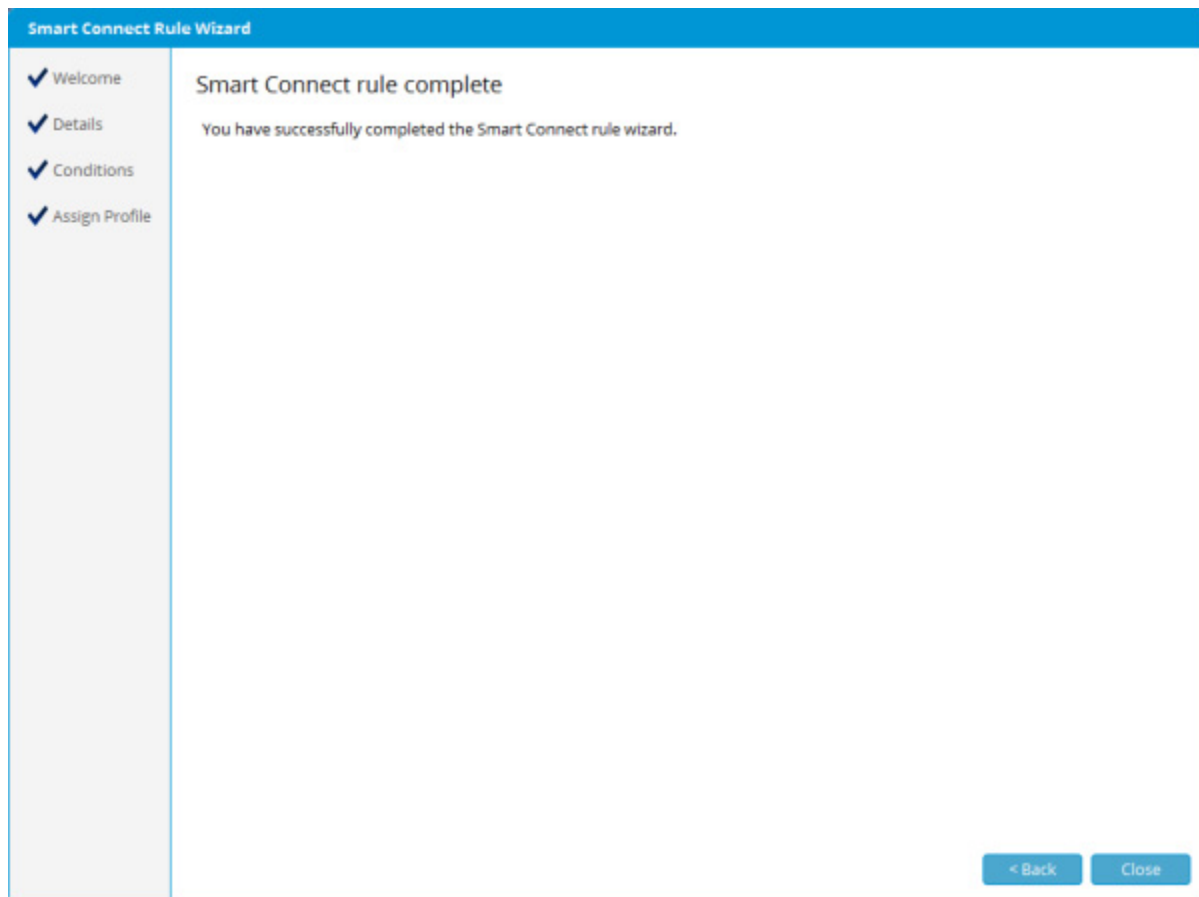
Wireless - select which Smart Connect profile to assign for Wireless profiles.

Note: FortiConnect supports multiple wired and wireless profiles.

10. Enable/Disable the check box to Allow users to continue using the open networks instead of running Smart Connect when they authenticate.

11. Enable/Disable the check box to Use Apple Configuration profiles for clients running OS X 10.7 or greater.

12. Click next once you have finished. You have now successfully created your Smart Connect Policy.



Editing a Smart Connect Policy

1. From the FortiConnect Administration Interface go to Smart Connect --> Smart Connect Policy as shown below.

Smart Connect Policy

The Smart Connect policy defines which Smart Connect profiles are applied to each user.

Each Smart Connect policy is checked in the following order. First matched policy is applied and no other policies are checked.

Order	Name	Rule	Wired Profiles	Wireless Profiles	Enabled	Action
1	Rule One	account-group equals Default Account Group and Acct-Delay-Time equals 14	No Smart Connect			
2	Default	default rule	No Smart Connect			

- Click on the Edit Policy Icon next to the policy you wish to Edit.
- Repeat steps 4 - 10 in the Adding a Smart Connect Policy section to make any changes.




Deleting a Smart Connect Policy

- From the FortiConnect Administration Interface go to Smart Connect --> Smart Connect Policy as shown below.

Smart Connect Policy

The Smart Connect policy defines which Smart Connect profiles are applied to each user.

Each Smart Connect policy is checked in the following order. First matched policy is applied and no other policies are checked.

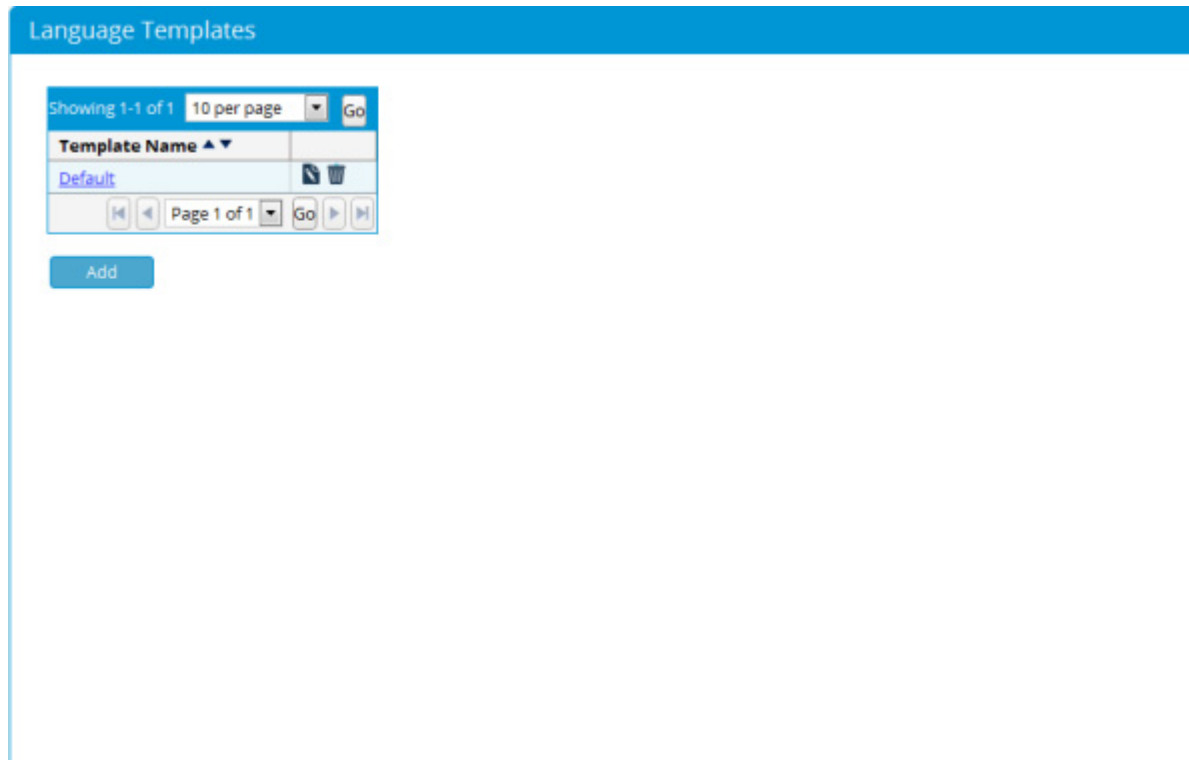
Order	Name	Rule	Wired Profiles	Wireless Profiles	Enabled	Action
1	Rule One	account-group equals Default Account Group and Acct-Delay-Time equals 14	No Smart Connect			 
2	Default	default rule	No Smart Connect			

Save Order
Add

- Click on the Bin Icon next to the Policy you wish to delete.
- Click on yes to confirm.

Language Templates

Administrators can add and remove different language templates for different network clients.



- Click on the Default link to check the language, you will open up a screen as shown below detailing different platforms.

Adding a Language Template

Language Templates: Default

Android Windows Linux Mac OSX Apple IOS

Application Logo: No file chosen

Username Label:

Password Label:

Login Button:

Connecting:

Failed to Connect to Network:

Connected:

Connected Message:
%ssid% will be replaced by network SSID

Invalid Credentials:

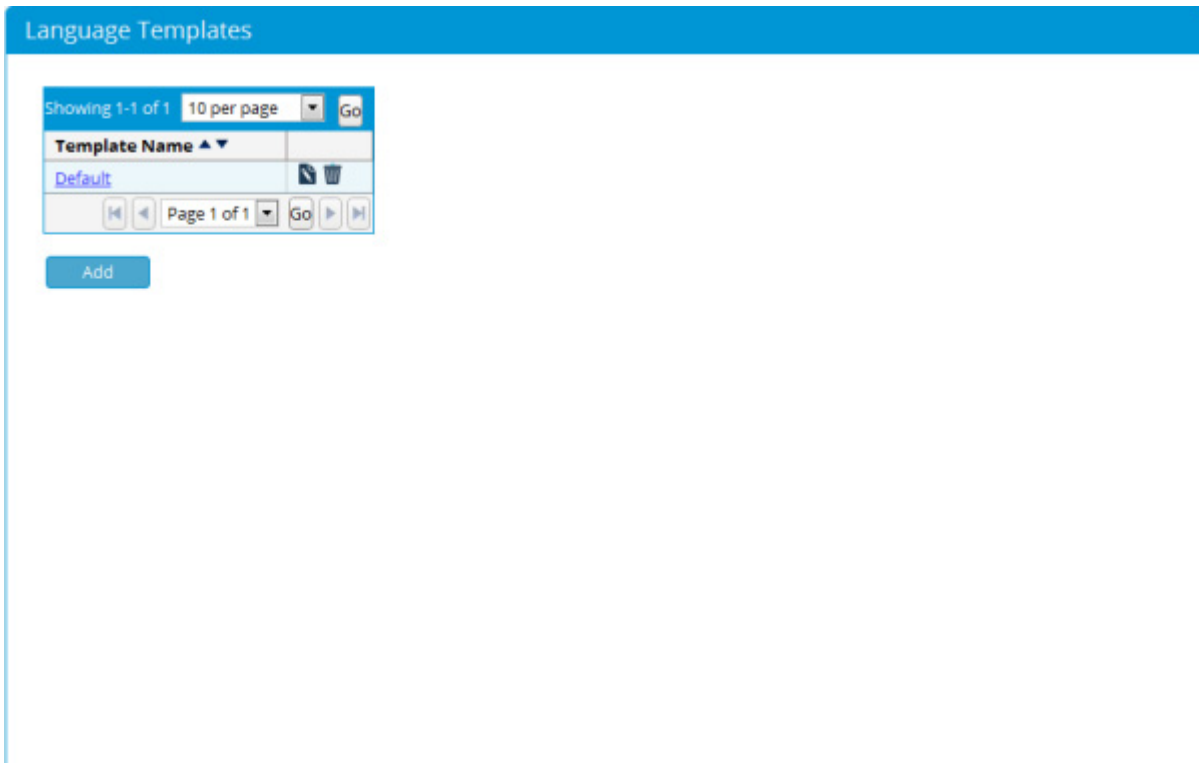
- From the tabs select which Platform you wish to edit.
- To upload an application logo, click on choose file and select a logo from your files.
- Edit any language as necessary by changing the text in the fields provided.

Note: Different platforms may have different fields.

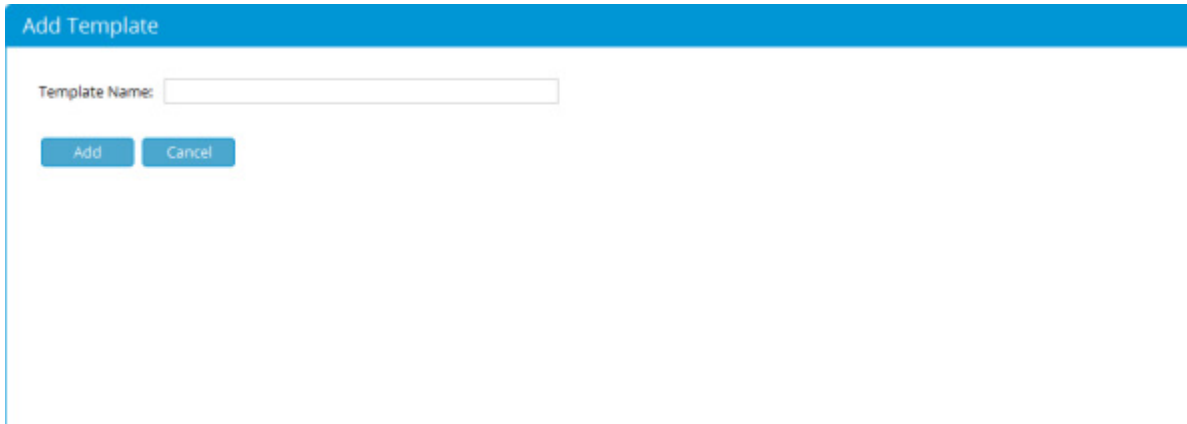
- Click on Save to keep any changes made to the text.

Adding a Language Template

To add a Language Template go to Smart Connect --> Language Templates from the Administration interface.



Click on Add



Enter the name of your Template and click on Add once complete.

Language Templates: Meru Template

✓ Template "Meru Template" created based on default template

Android Windows Linux Mac OSX Apple IOS

Application Logo: No file chosen

Username Label:

Password Label:

Login Button:

Connecting:

Failed to Connect to Network:

Connected:

Connected Message:

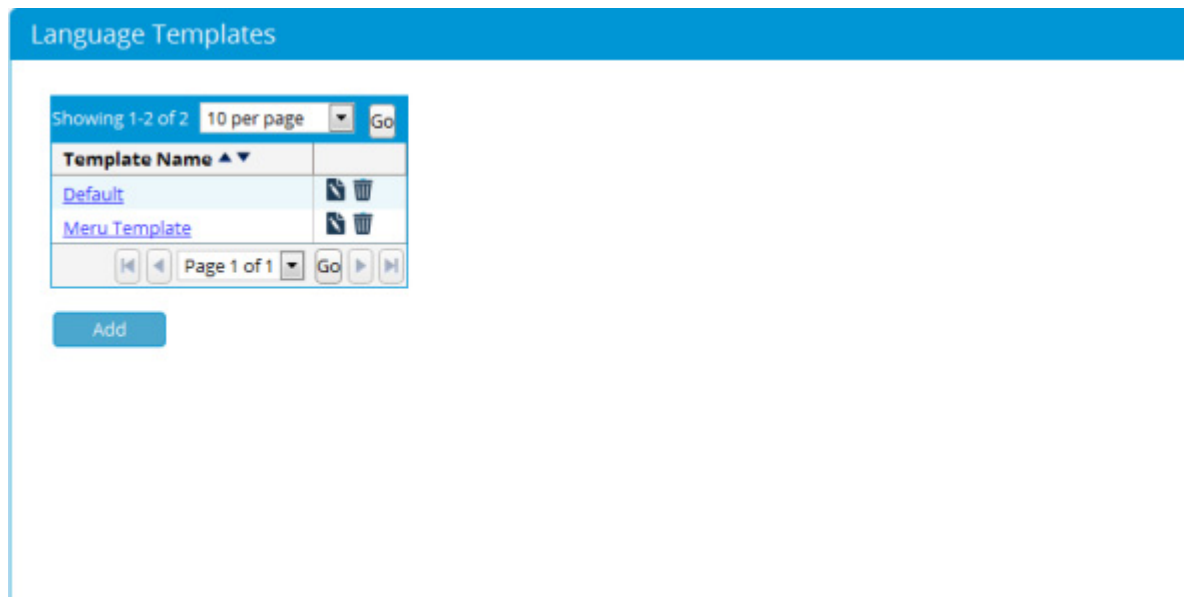
Invalid Credentials:

Your template will be created and be based on the already pre-defined Default template and will automatically direct you to the Android tab.

- To upload a logo click on the Choose File button and upload a logo from your files.
- Change the text in the fields provided.
- To change the text on any other platforms then click on the appropriate tab and make your changes.
- Click Save once completed.

Editing a Language Template

To edit a template, go to Smart Connect --> Language Templates from the Administration database as shown below.

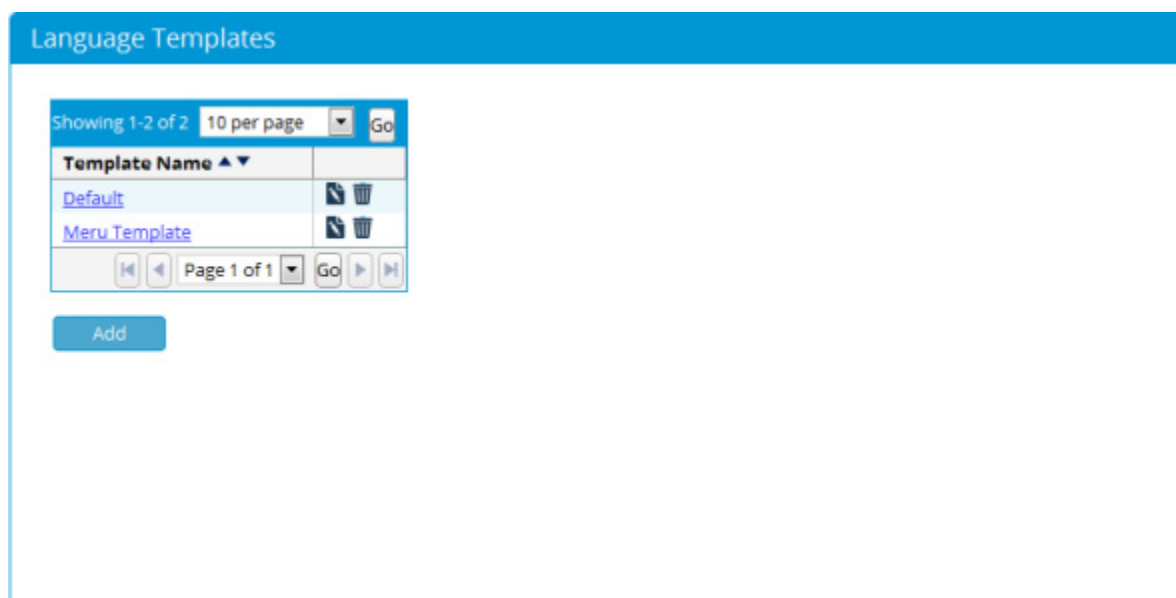


Click on the Edit icon next to the Template you wish to edit.

Make any necessary changes and click on Save once completed.

Deleting a Language Template

To delete a Language Template go to Smart Connect --> Language Templates from the Administration interface.



Click on the Bin icon next to the template you wish to delete and click on yes to confirm deletion.

Code Signing Certificates

FortiConnect supports the upload of Authenticode Code Signing Certificates & CSR / Key generation. This allows the Windows Smart Connect executable to be signed on generation and reduces the number of security warnings that appear when it's downloaded and run.

If certificates are uploaded, the executable will be 'published' by the organization name specified on the certificate and no longer show as having an 'unknown publisher'.

The nature of Windows messages should now be informational alerts rather than security warnings.

Note: Contact should be made to the Certificate Authority with a view to purchasing any relevant certificates, in this case a Microsoft Authenticode Code Signing Certificate is required. Depending on the Certificate Authority you approach, they may require a CSR (Certificate Signing Request), you can create the CSR following instructions in the next section.

1. From the FortiConnect Interface go to Smart Connect -->Code Signing Certificates as shown below.

Code Signing Certificates

Certificate Signing Request

[Create CSR](#)

[Download CSR](#)

Download

[Download Current Certificate](#)

[Download Current Private Key](#)

[Download Current Combined Certificate & Private Key](#)

Upload Certificate

Upload Code Signing Certificate: No file chosen

Upload Certificate and Private Key

Upload Code Signing Certificate: No file chosen

Upload Code Signing Private Key: No file chosen

Upload Combined Certificate & Private Key (*.pfx, *.p12)

Upload Combined Code Signing File: No file chosen

Passphrase:

Leave blank if no passphrase associated with file

2. From here we can -

Certificate Signing Request

- Create CSR - Create a CSR (detailed further below)
- Download CSR - Download the CSR file

Download

- Download Current Certificate - Downloads the current certificate
- Download Current Private Key - Download the current private key
- Download Current Combined Certificate & Private Key - Download the current combined certificate and private key

Upload Certificate

- Upload Code Signing Certificate - Click on Choose File and select and upload a code signing certificate

Upload Certificate and Private Key

- Upload Code Signing Certificate - Click on Choose File and select and upload a code signing certificate

- **Upload Code Signing Private Key** - Click on Choose File and select and upload a code signing private key

Upload Combined Certificate and Private Key (*.pfx, *.p12)

- **Upload Combined Code Signing File** - Click on Choose File and select and upload the combined certificate and private key.
- **Passphrase** - Enter the passphrase if one is associated with the combined certificate and private key file.

3. Click on Upload to upload certificates.

Create CSR

If you are required to create a CSR then click on the Create CSR link and you will be presented with the screen below.

Create CSR

Code Signing CSR

Organization:
Legal name of your Organization without abbreviation, including any suffixes e.g. Inc, Corp etc.

Email:

Organizational Unit (Section):

Locality (e.g. City):

State or Province:

Country:

Private Key Regeneration

WARNING: Regenerating the private key will invalidate any existing code signing certificates

Regenerate Private Key: ☒

1. Using the fields provided enter the following required information -
 - **Organization** - The legal name of your organization
 - **Email** - Email address
 - **Organizational Unit (Section)** - Organizational Unit
 - **Locality** - City or Area
 - **State or Province** - State or Province
 - **Country** - From the drop down menu select your country.

2. Place a check in the Regenerate Private Key checkbox should you wish to regenerate the private key.
3. Click on Create to create your CSR

Device Logs

Smart Connect uses Device Logs as a troubleshooting functionality for devices connected to the network using Smart Connect.

1. To view the Device Logs go to Reports & Logs --> Smart Connect Device Logs on the FortiConnect Administration Interface as shown below.

Smart Connect Device Logs

Username: Platform: All

Between: 1 Dec 2014 00:00 And: 2 Dec 2014 23:59

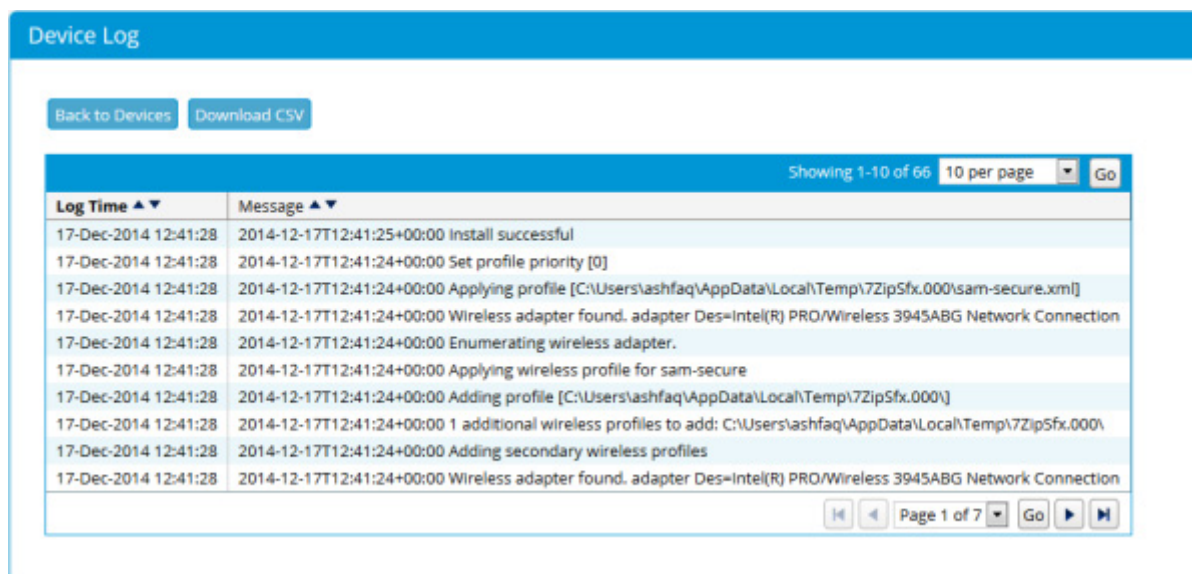
Run

10 per page Go

Username	Platform	Model	Time	Device Logs
No Records Found				

2. Using the fields provided you can tailor your search as defined:-
 - Username - If you are searching for a specific user enter the username here.
 - Platform - From the dropdown menu select which platform you wish to perform your search on.
 - Between - Enter the date and time you wish to start your search from.
 - And - Enter the date and time you wish to end your search from.

3. Click on Run to perform the search.
4. Once the search has been completed, the table will populate with your search results, to view the Device Logs from a specific search click on the View link next to the result as shown below.



The screenshot shows a web interface titled "Device Log". At the top, there are two buttons: "Back to Devices" and "Download CSV". Below these is a table with two columns: "Log Time" and "Message". The table displays 10 log entries. At the bottom right of the table, there is a pagination control showing "Page 1 of 7" and "Go" buttons.

Log Time ▲▼	Message ▲▼
17-Dec-2014 12:41:28	2014-12-17T12:41:25+00:00 Install successful
17-Dec-2014 12:41:28	2014-12-17T12:41:24+00:00 Set profile priority [0]
17-Dec-2014 12:41:28	2014-12-17T12:41:24+00:00 Applying profile [C:\Users\ashfaq\AppData\Local\Temp\7ZipSfx.000\sam-secure.xml]
17-Dec-2014 12:41:28	2014-12-17T12:41:24+00:00 Wireless adapter found. adapter Des=Intel(R) PRO/Wireless 3945ABG Network Connection
17-Dec-2014 12:41:28	2014-12-17T12:41:24+00:00 Enumerating wireless adapter.
17-Dec-2014 12:41:28	2014-12-17T12:41:24+00:00 Applying wireless profile for sam-secure
17-Dec-2014 12:41:28	2014-12-17T12:41:24+00:00 Adding profile [C:\Users\ashfaq\AppData\Local\Temp\7ZipSfx.000\]
17-Dec-2014 12:41:28	2014-12-17T12:41:24+00:00 1 additional wireless profiles to add: C:\Users\ashfaq\AppData\Local\Temp\7ZipSfx.000\
17-Dec-2014 12:41:28	2014-12-17T12:41:24+00:00 Adding secondary wireless profiles
17-Dec-2014 12:41:28	2014-12-17T12:41:24+00:00 Wireless adapter found. adapter Des=Intel(R) PRO/Wireless 3945ABG Network Connection

5. The Device log will display the:-
 - Log Time - Date and Time of the log
 - Message - Log message.
6. Click on the Download CSV button if you wish to download the logs as a CSV file.
7. Click on the Back to Devices button to perform another search.

SCEP and User Certificate Authorities

FortiConnect allows distribution of certificates to devices when they are authenticated onto the network. This can be done in a few different ways.

- If you wish to generate user certificates on an external server (e.g. Active Directory) then you can add an entry in Smart Connect--> SCEP Servers.
- You can also generate certificates internally on the FortiConnect, you may configure this in Smart Connect --> User Certificate Authorities.

- Certificates can be uploaded manually during setup in Network Access Policy --> Authentication Policy.

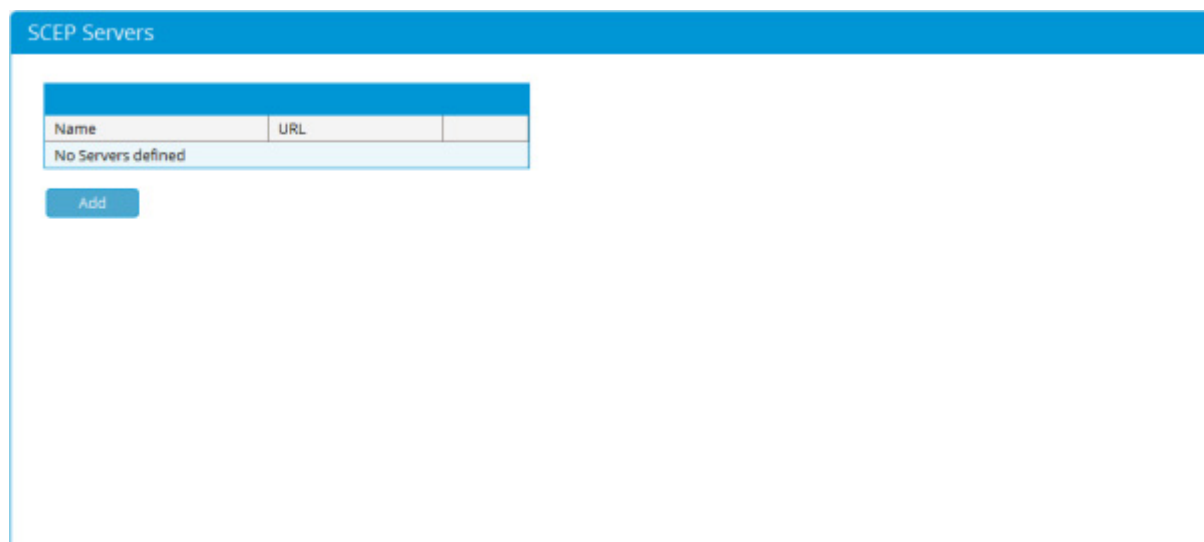
To allow authentication with a user certificate you must edit a Network Access Policy by going to Network Access Policy --> Authentication Policy. and select the certificate source(s) that are associated with the policy during setup.

When the network user requests a Smart Connect profile, a user certificate is generated, this is done by selecting EAP-TLS as an EAP type in a Smart Connect Profile using the wizard in **Smart Connect --> Smart Connect Profiles**, you may then choose one of the above certificate sources so when the network user requests a Smart Connect profile the user certificate is generated.

The sections below detail how to Add a **SCEP Server** and how to generate Certificates internally using **User Certificate Authorities**.

Adding a SCEP Server

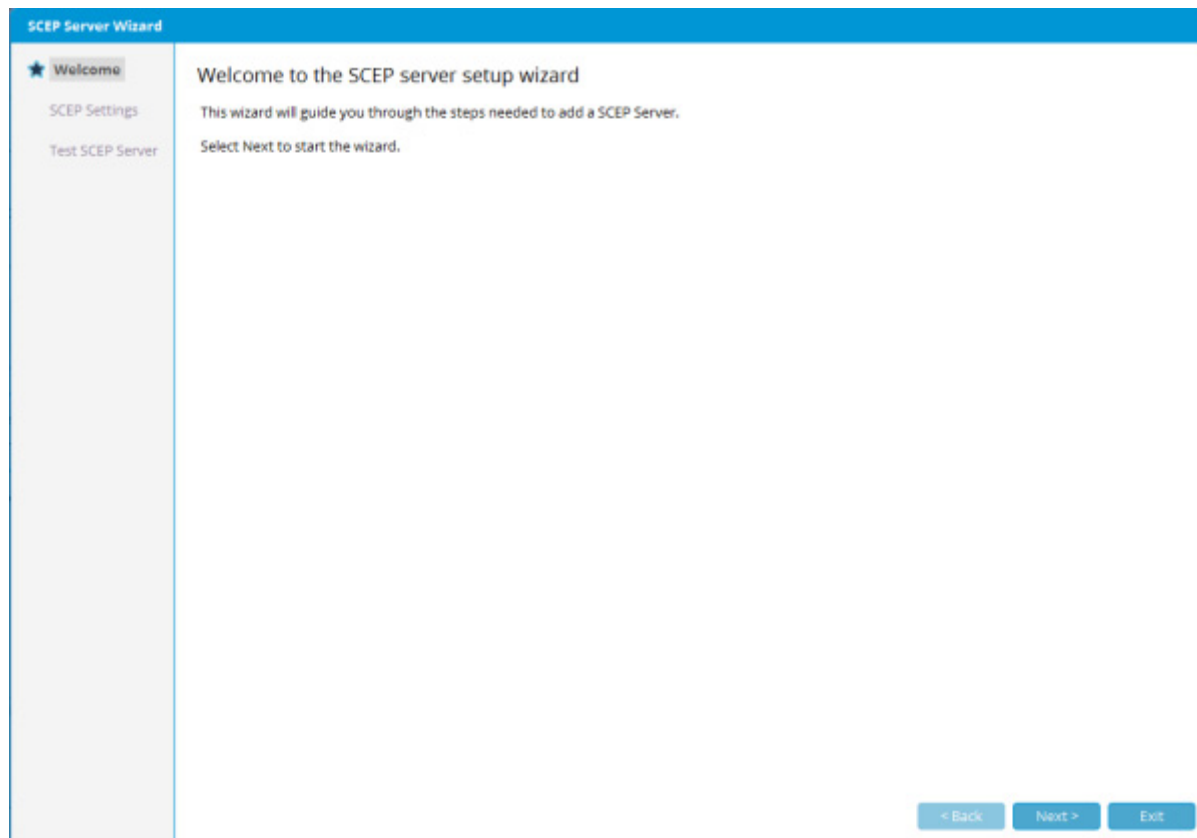
If you wish to generate user certificates on an external server (e.g. Active Directory) then you can add an entry from the FortiConnect Interface at Smart Connect--> SCEP Servers.



Name	URL
No Servers defined	

Add

1. To add a SCEP server click on the Add button to open up the SCEP Server Wizard.

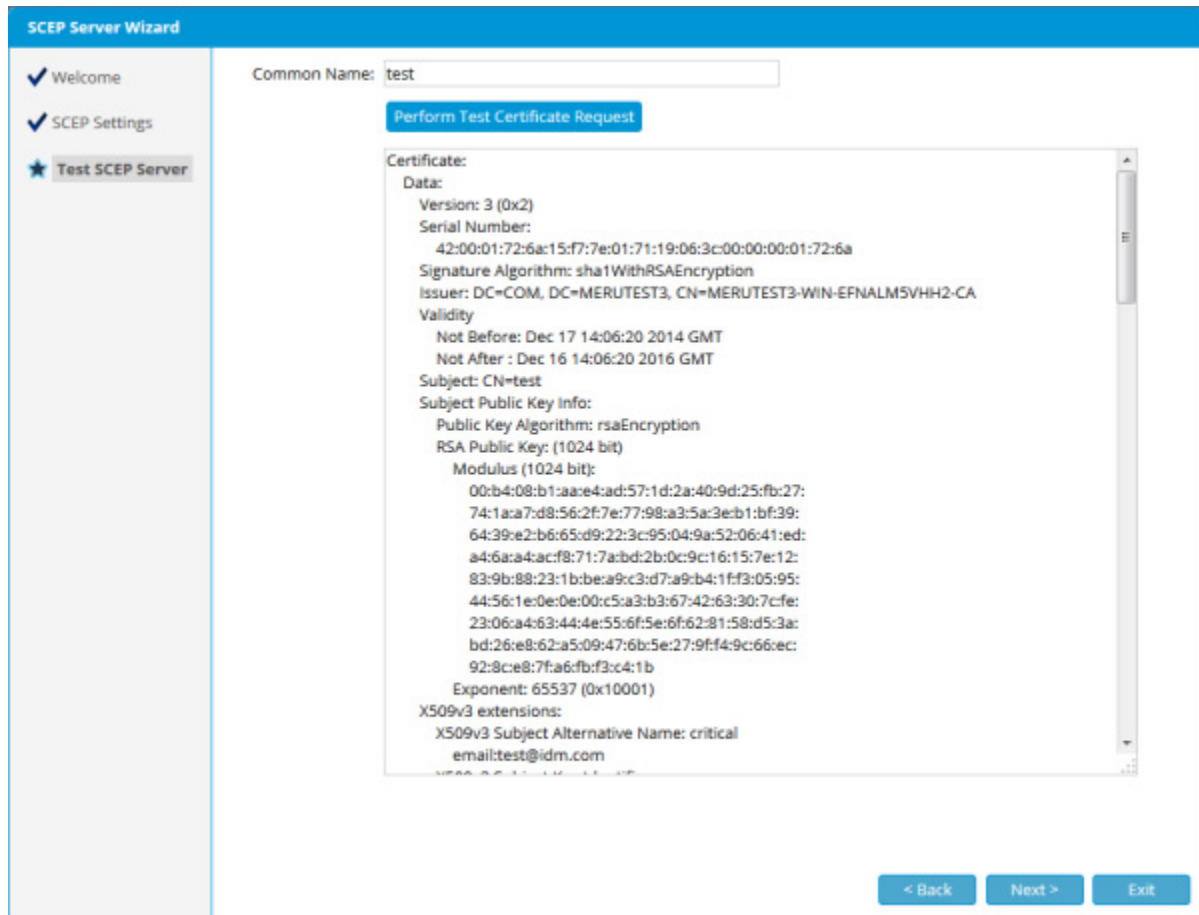


2. Click on Next to enter the SCEP Server settings as shown below.

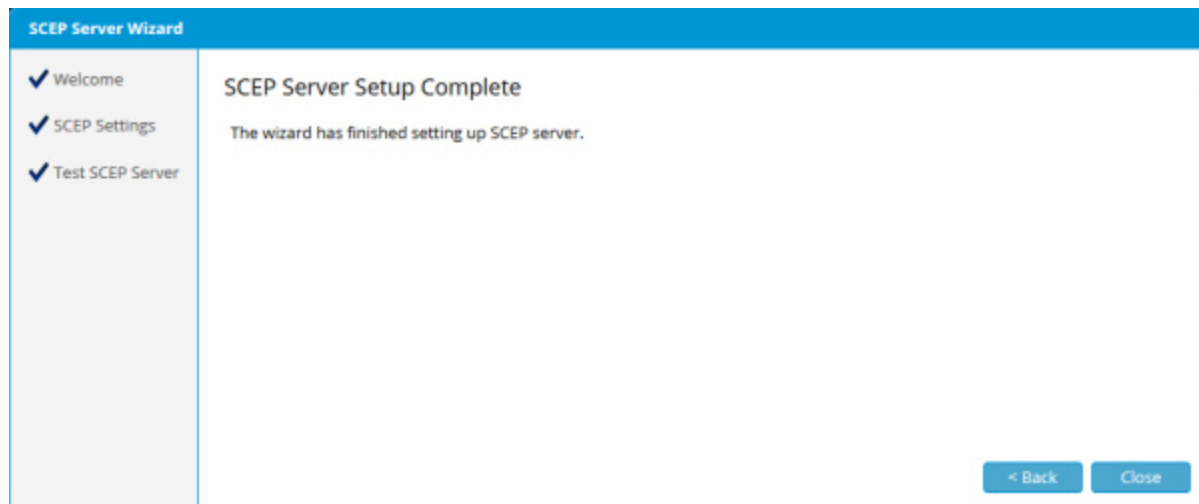
The screenshot shows the 'SCEP Server Wizard' window. On the left is a sidebar with three options: 'Welcome' (checked), 'SCEP Settings' (selected with a star), and 'Test SCEP Server'. The main area contains configuration fields for the SCEP server. At the bottom right are three buttons: '< Back', 'Next >', and 'Exit'.

Field	Description / Notes
Name:	
SCEP URL:	
CA Identifier:	Not required if connecting to NDES on a Windows server.
Challenge Password:	Required if connecting to NDES on a Windows server. If left blank the user's current password is used when generating their client certificate.
Key Size:	1024 (dropdown menu). The user's certificate will be generated with this key size.
OCSP Responder URL:	Optional. An OCSP request will be sent to this URL to validate a user's certificate when authenticating.

3. In the fields provided, enter the following -
 - Name - Enter the Name of the SCEP Server
 - SCEP URL - Enter the URL of the SCEP Server (HTTP only)
 - CA Identifier - Enter the CA Identifier for your SCEP Server (note that this is not required if connecting to NDES on a windows server)
 - Challenge Password - Required if connecting to NDES on a Windows Server. If left blank then the users current password is used when generating their client certificate.
 - Key Size - From the drop down menu select whether the key size should be 1024 or 2048 bits
 - OCSP Responder URL - Optional Field, but if required enter the URL to send an OCSP request for validating user certificates when authenticating.
4. Click on Next to continue.
5. You can then perform a test to confirm the certificate request and check your settings are ok, click on Perform Test Certificate Request on the Test SCEP Server screen as shown below.

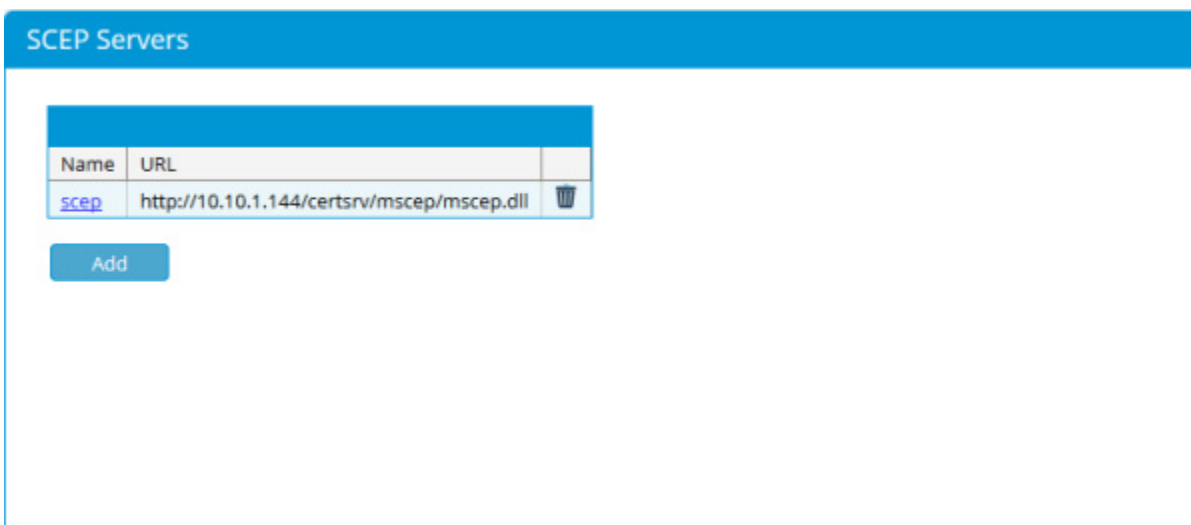


6. Your results will populate the empty field as shown above.
7. Click on Next to complete the setup.



Editing a SCEP Server

If you wish to EDIT a SCEP Server goto Smart Connect--> SCEP Servers on the FortiConnect Interface



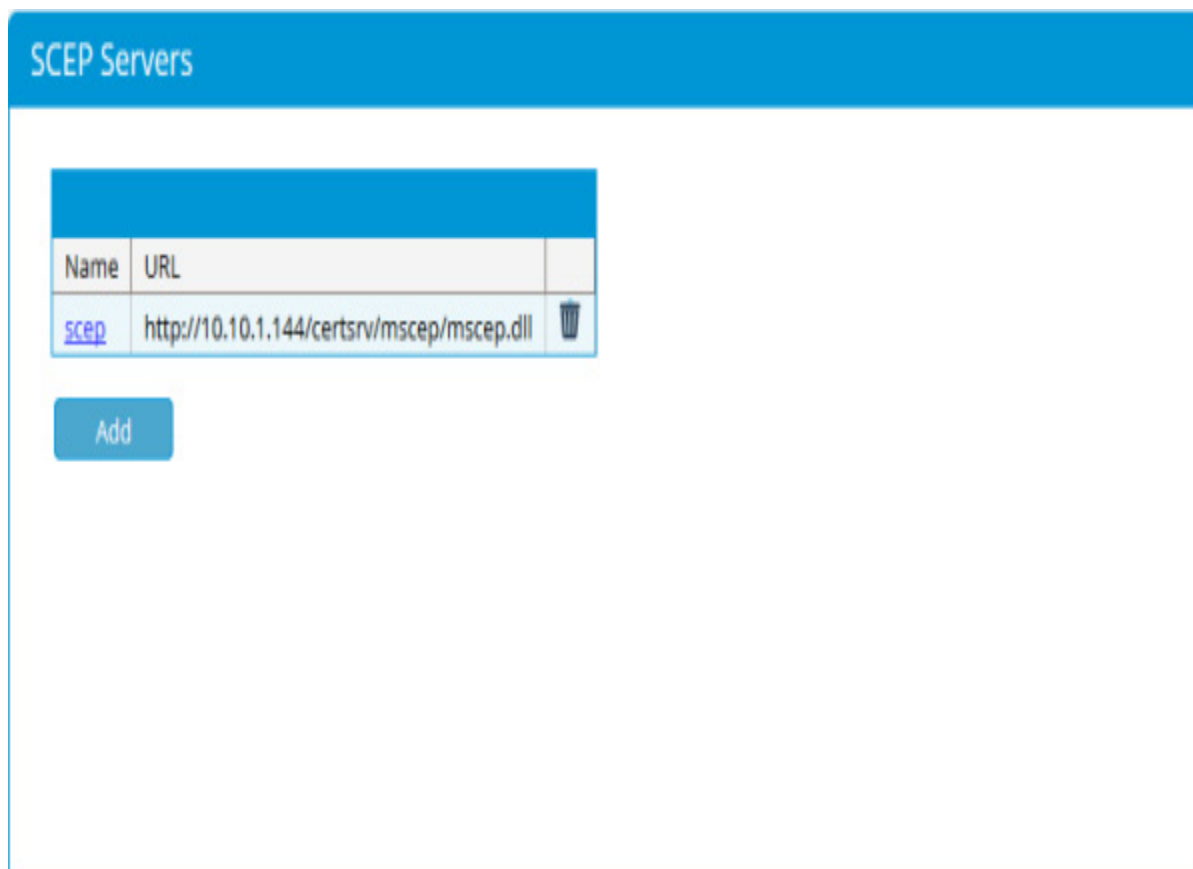
1. Click on the Name of the SCEP Server you wish to Edit and perform the appropriate changes.
2. In the fields provided, enter the following -
 - Name - Enter the Name of the SCEP Server

- SCEP URL - Enter the URL of the SCEP Server (HTTP only)
- CA Identifier - Enter the CA Identifier for your SCEP Server (note that this is not required if connecting to NDES on a windows server)
- Challenge Password - Required if connecting to NDES on a Windows Server. If left blank then the users current password is used when generating their client certificate.
- Key Size - From the drop down menu select whether the key size should be 1024 or 2048
- OCSP Responder URL - Optional Field, but if required enter the URL to send an OCSP request to for validating user certificates when authenticating.

3. Click on Next to continue.

Deleting a SCEP Server

If you wish to Delete a SCEP Server goto Smart Connect--> SCEP Servers on the FortiConnect Interface



1. Click on the Bin icon next to the SCEP Server you wish to Delete.
2. Click on Ok to confirm.

Adding a User Certificate Authority

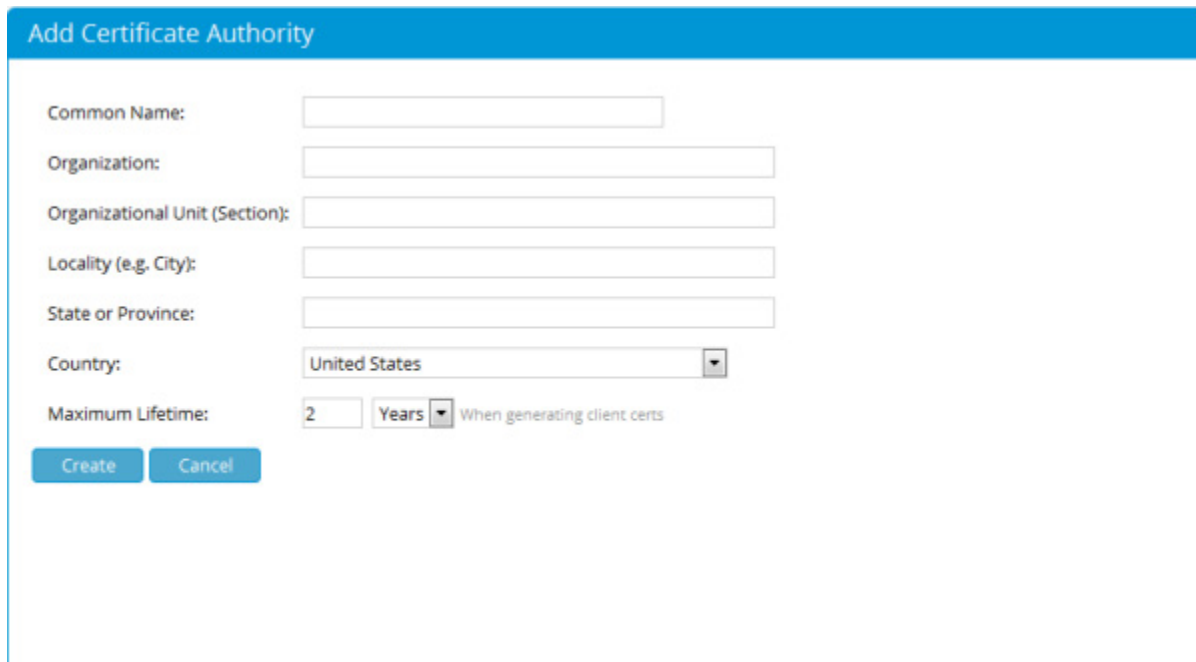
Certificates can be generated internally on the FortiConnect, you may configure this in Smart Connect --> User Certificate Authorities.

User Certificate Authorities

Common Name	Issued Certificates	Max Lifetime	
No Certificate Authorities defined			

Create

1. To Add a Certificate Authority click on the Create button.



Add Certificate Authority

Common Name:

Organization:

Organizational Unit (Section):

Locality (e.g. City):

State or Province:

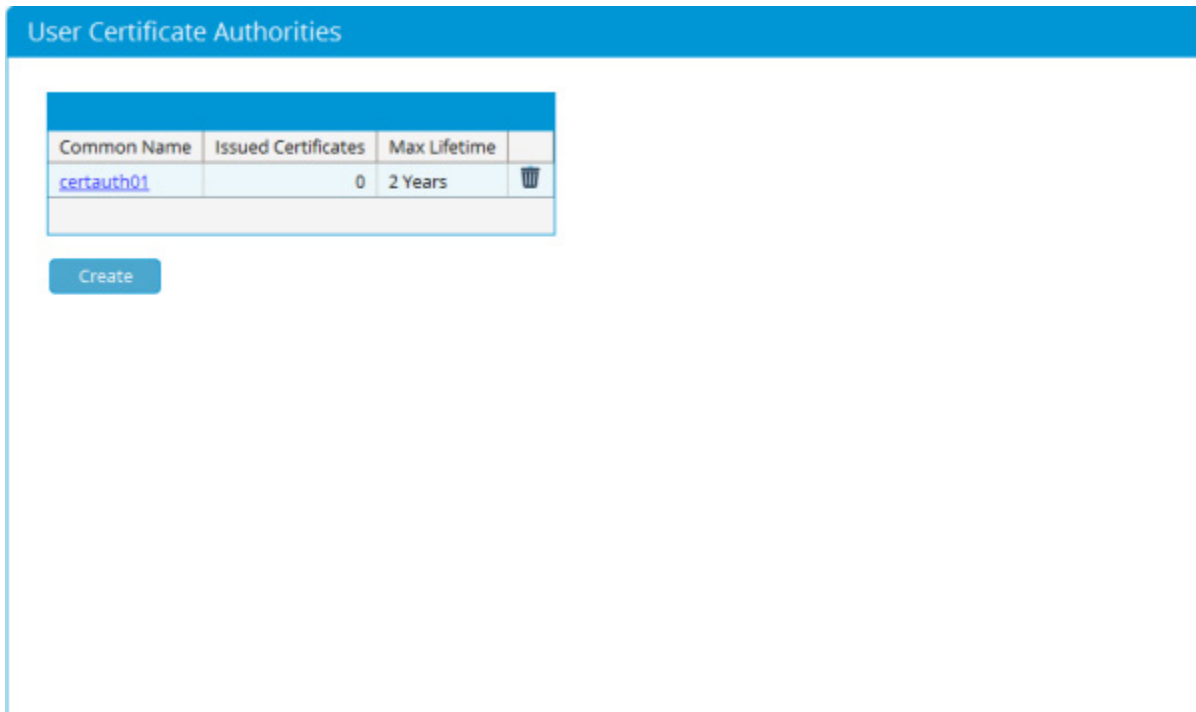
Country:

Maximum Lifetime: When generating client certs

2. In the fields provided, enter the following -
 - Common Name - Common Name of the Certificate Authority
 - Organization - Organization
 - Organization Unit - Organization Unit or Section of the Certificate Authority
 - Locality - Locality of the Certificate Authority
 - State or Province - State or Province of the Certificate Authority
 - Country - From the drop down menu select the country of the Certificate Authority
 - Maximum Lifetime - Use the drop down menus to define the Maximum Lifetime of any generated certificate.
3. Click on Create once complete

Editing a User Certificate Authority

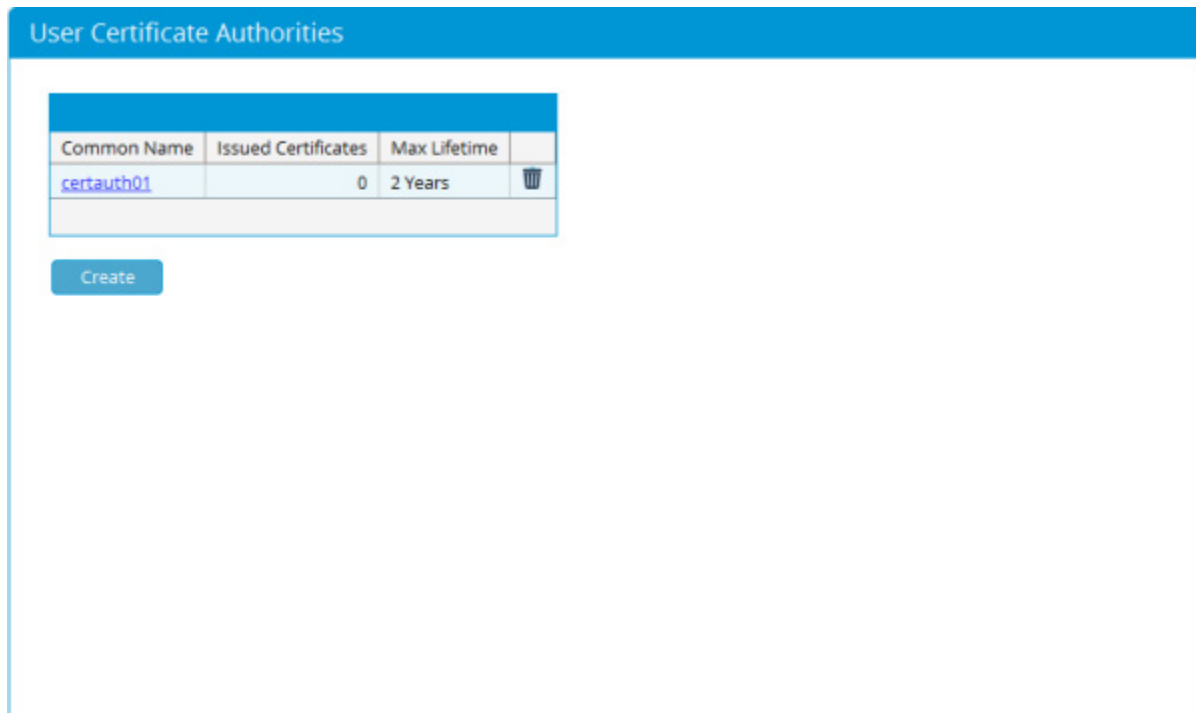
If you wish to Edit a User Certificate Authority, go to Smart Connect --> User Certificate Authorities.



1. Click on the Name of the User Certificate Authority you wish to Edit and perform the appropriate changes.
2. In the fields provided, enter the following -
 - Common Name - Common Name of the Certificate Authority
 - Organization - Organization
 - Organization Unit - Organization Unit or Section of the Certificate Authority
 - Locality - Locality of the Certificate Authority
 - State or Province - State or Province of the Certificate Authority
 - Country - From the drop down menu select the country of the Certificate Authority
 - Maximum Lifetime - Use the drop down menus to define the Maximum Lifetime of any generated certificate.
3. Click on Create once complete

Deleting a User Certificate Authority

If you wish to Delete a User Certificate Authority goto Smart Connect--> User Certificate Authority on the FortiConnect Interface



1. Click on the Bin Icon next to the Name of the User Certificate Authority you wish to Delete.
2. Click on Ok to confirm.

Note: EAP-TLS & PEAP/EAP-TLS cannot be provisioned automatically on Windows XP Clients by Smart Connect.

Replication and High Availability

To provide high availability, the FortiConnect solution can be configured so it is part of a cluster with all members of the cluster synchronizing their databases between one another. This provides the ability for the solution to carry on working in the event of loss of connectivity or failure to a single unit.

High availability is provided in an active/active scenario, where all FortiConnect can service requests from sponsors or network devices at the same time. This capability also allows you to load balance the requests between the boxes.

Note: Not all system settings are replicated. Refer to Data Replicated to review which settings are not replicated.

Note: For load balancing, external load balancers must be used to load balance the web interface. RADIUS requests can also be load balanced via external load balancers or by configuration.

Note: Replication is only supported on FortiConnect servers running identical versions of software. This chapter includes the following sections:

- Configuring Replication
- Configuring Provisioning
- Replication Status
- Recovering from Failures
- Deployment Considerations

Cluster Configuration

FortiConnect supports multiple instances of IDM in the cluster. Each system is fully active at any point in time and can receive and respond to requests with no dependence on any other system in the cluster.

Note: You will need to set up one of your FortiConnect systems as the Registration Server then add any other Normal Servers afterwards.

Note: To enable replication, all servers in a cluster must be able to validate each others certificate, to do this, each server will need a certificate signed by a trusted CA and can be uploaded to Server --> SSL Settings before you continue.

Note: In previous versions of FortiConnect files/certificates/themes would have to be uploaded individually to each box in the cluster, however, in FortiConnect 13.6 an upload to a FortiConnect will automatically be applied to all others in the cluster at the same time.

Cluster Configuration

1. From the FortiConnect Interface go to Server --> Cluster Configuration and you will be presented with the Setup screen as shown below.

Cluster Configuration

Setup

Meru Connect supports multiple instances of MCT in the cluster. Each instance is fully active at any point in time and can receive and respond to requests with no dependence on any other instance in the cluster.

- Disabled - Cluster support is disabled.
- Registration Server - In each cluster one and only one system should be enabled as Registration Server. All other servers contact the Registration Server during initial setup to learn about all other servers in the cluster.
- Normal Server - Each other server should be setup as a Normal server.

Once initial setup has taken place all servers behave identically.

Server Mode: ☐ Disabled ☐ Registration Server ☒ Normal Server

Registration Server:
Hostname or IP address

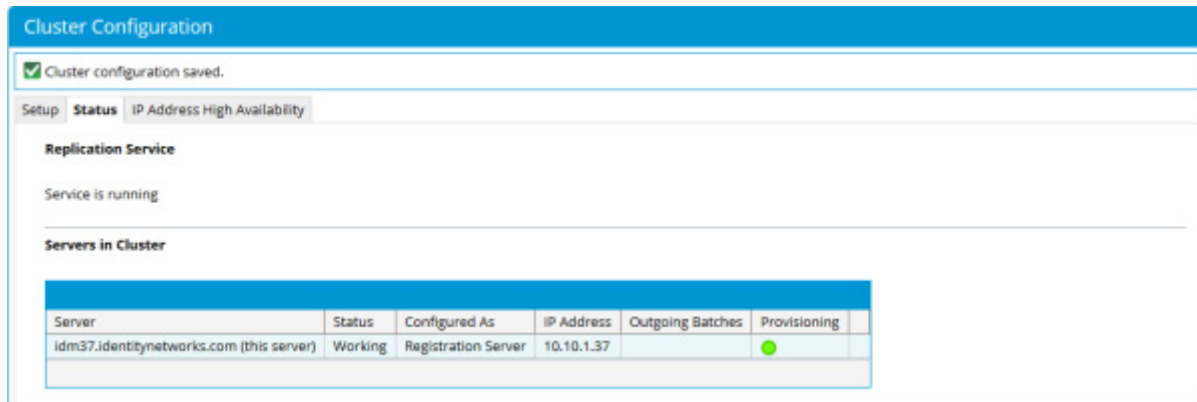
Shared Secret: Confirm:
The Shared Secret should be the same on all servers in the cluster. It is used to authenticate servers to each other.

Validate Certificate common name: ☒ Certificates can be uploaded in [Server > SSL Settings](#)
SSL is used to encrypt connections between servers, you can choose to validate the certificates presented by each IDM.

Save

2. There are 3 options to choose from for server mode -
 - Disabled - Cluster support is disabled.
 - Registration Server - In each cluster one and only one system should be enabled as Registration Server. All other servers contact the Registration server at initial setup to learn about all other servers in the cluster.
 - Normal Server - Each server should behave identically.
3. Once you have made your selection enter the appropriate details in the fields provided.
 - Registration Server - If Normal Server Mode has been selected, enter the Hostname or the IP Address of your chosen Registration Server.
 - Shared Secret - Enter the Shared Secret and Confirm. The Shared Secret should be the same for all servers in the cluster.
 - Validate Certificate Common Name - SSL is used to encrypt connections between servers, you can select this option to validate the certificates presented by each IDM.
4. Click on Save to continue.
5. Your screen will change and some extra tabs will appear along the top as shown below.

Note: When adding a new server other than the Registration Server, all data will be wiped from that server when it is added to the cluster.



6. You will then be taken to the Status Tab which will detail -
- Replication Service - Whether your replication service is running.
 - Servers in Cluster - A list of servers in your cluster, their status, what they have been Configured As, its IP Address, any Outgoing Batches and Provisioning.

IP Address High Availability (VRRP)

IP Address high availability allows a single virtual IP Address to be defined and shared between two FortiConnect Servers so that in the event of failure, the Virtual IP address is picked up by the backup server of the pair which then continues to service requests.

FortiConnect provides High Availability between 2 nodes in a local cluster belonging to the same subnet by using the VRRP Protocol. IP Address High Availability can be performed by following the steps below.

1. From the FortiConnect Interface go to Server --> Cluster Configuration and click on the IP Address High Availability tab as shown below.

The screenshot shows the 'Cluster Configuration' window with the 'IP Address High Availability' tab selected. The window has a blue header bar with the title 'Cluster Configuration'. Below the header, there are two tabs: 'Setup' and 'Status'. The 'Setup' tab is active. The main content area contains a blue information icon followed by text explaining that IP Address High Availability uses the VRRP protocol for active/backup services for a shared IP address. It also states that devices are configured to use this virtual IP address, which runs on the Master node by default, and that the Backup node will take over in the event of a Master node failure. Below this text, there is a status indicator showing 'Status: This server is currently inactive' with a grey circle. A checkbox labeled 'Enable VRRP:' is checked. Under the 'Server Settings' section, there is a 'Server Mode' dropdown menu set to 'Master', a 'Virtual IP Address' text input field, and a 'Shared Secret' text input field with a 'Confirm:' text input field next to it. At the bottom left, there are 'Save' and 'Cancel' buttons.

2. IP Address High Availability uses the VRRP protocol to allow two FortiConnects to provide active/backup services for a shared IP Address. Devices are configured to use this virtual IP Address which by default runs on the Master node. In the event of the Master node failing the Backup node will take over the IP address and service requests.
 - Enable VRRP - Check this box to enable VRRP settings.
 - Server Mode - From the drop down menu select whether you wish to setup the Master or Backup mode.
 - Virtual IP Address - Enter the virtual IP address for the server.
 - Shared Secret - Enter and then confirm the shared secret for the server.
3. Click on Save once completed.
4. Once this has been completed the Server Status will change as shown on the screen below.

The screenshot shows the 'Cluster Configuration' window with a blue header. Below the header, a status bar indicates 'Settings saved & VRRP activated'. The main content area has tabs for 'Setup' and 'Status', with 'IP Address High Availability' selected. A blue information icon is followed by text explaining that IP Address High Availability uses the VRRP protocol for active/backup services. Below this, a status message states: 'Status: This server is currently active [as master] for virtual IP [10.10.1.199]' with a green circle icon. The 'Enable VRRP' checkbox is checked. Under the 'Server Settings' section, 'Server Mode' is set to 'Master'. The 'Virtual IP Address' field contains '10.10.1.199'. The 'Shared Secret' field is empty, with a 'Confirm' field next to it. A small note below the fields says 'Leave blank to keep existing password'. At the bottom are 'Save' and 'Cancel' buttons.

Configuring Provisioning

Certain operations should only be performed by one of the FortiConnects in the cluster, provisioning accounts on external devices and sending notifications to users are examples of such operations.

One FortiConnect should be defined as the provisioning node. The provisioning server will perform the provisioning by default. If an FortiConnect is not the provisioning server, it checks the status of the provisioning server and the other servers in the cluster. If it fails to contact the provisioning server and fallback servers three times, then it will assume these are down and will then perform the provisioning. This process happens every minute when the provisioning service runs.

1. From the administration interface of the cluster registration server, select Server > Cluster Configuration--> Status.
2. Click on the grey circle in the Provisioning column to specify the server should handle provisioning.
3. The circle should turn green.

Note: Only one of the servers should have Provisioning enabled, otherwise you may get errors when creating or deleting accounts twice.

Replication Status

At any time, you can check the replication status of the FortiConnects. This is useful to make sure replication is happening as set.

From the administration interface, select Server > Cluster Configuration --> Status.

Here you can check the status of the replication service, list the FortiConnects in the cluster, identify the provisioning server and see the number of records waiting to be replicated from the FortiConnect you are connected to the remaining nodes.

Recovering from Failures

Network Connectivity

When the network connectivity between two FortiConnects fails, the FortiConnect stores up to 1GB of changes. When connectivity is restored, if the amount of changes is less than 1GB, they will synchronize with each other. If more than 1GB of changes are stored, the FortiConnect stops the replication process and you need to setup replication again.

Device Failure

If one of the FortiConnects in a cluster fails and needs to be replaced, you should simply join the replacement FortiConnect to the cluster. If the FortiConnect that failed was the registration server, you will need to promote one of the remaining servers in the cluster to the position of registration server before joining the new FortiConnect to the cluster.

To elevate one FortiConnect to the position of registration server you will need to -

1. From the administration interface of the Identity Manager that will be the new registration server you will need to, select Server > Cluster Configuration--> Setup as shown below.
2. Set the Server Mode to Registration Server.
3. Click Save.

Deployment Considerations

Connectivity

The FortiConnects need to be provided with IP connectivity between the units. Fortinet recommends making the network path between the devices resilient so that synchronization can always be performed. However, if the devices are disconnected, they will continue to function and store changes until they are connected back together and can re-establish communication. At this point, they will re-synchronize databases.

Depending on the amount of activity that your FortiConnect performs, you need to make sure that there is enough bandwidth between the servers to enable synchronization to occur as rapidly as possible.

You can test connectivity by creating a large number of accounts and watching how quickly the appliances synchronize by watching the status on the replication.

Load Balancing

Web Interface

Sponsor and Administration sessions can be serviced by both FortiConnects when configured for replication. However, the FortiConnect does not perform any redirection or automatic load balancing of requests.

To enable requests to both FortiConnects concurrently, you must implement an external load balancing mechanism. Options include:

- Network based Load Balancing— devices can be used to load balance web requests to the FortiConnects. The only requirement for the load balancing is that clients are serviced by the same FortiConnect for their entire session. Individual requests cannot be load balanced between servers, as the FortiConnect does not replicate sponsor/admin session information to reduce bandwidth requirements. The most common method of achieving this is sticking connections to the same FortiConnect based upon source IP address.
- DNS Round robin—Using your DNS server, configure the domain name of the FortiConnect to return all IP addresses for the FortiConnect in a round-robin configuration. This method does not provide failover between appliances in the event of a failure.

- Publishing multiple URLs—This allows each user to choose the server they want to use.

RADIUS Interface

The RADIUS interface on either FortiConnect can take requests at the same time.

Fortinet recommends configuring one to be the primary for some RADIUS clients and another FortiConnect to be the primary for the other RADIUS clients. For failover, the RADIUS clients can have secondary RADIUS servers defined as another FortiConnect, if they support configuration of two servers.

Data Replicated

FortiConnect Replication replicates data that is stored in the database between all FortiConnects in the cluster. The following information is not replicated and is locally defined on each FortiConnect.

- Email settings—SMTP Server
- Network settings
 - Domain name
 - Hostname
 - IP Address
 - Subnet mask
 - Default gateway
 - Nameserver 1
 - Nameserver 2
- Date/Time settings
 - Date Time Locale
 - NTP server 1
 - NTP server 2
- SSL settings
 - SSL Certificate
 - Root CA Certificate
 - Private key
- Backup
 - Max number of backups
 - Frequency
 - FTP settings

Management, Logging and Troubleshooting

This chapter describes the following:

- Dashboard
- SNMP Configuration
- System Logging
- RADIUS Authentication Logs
- User Accounts
- RADIUS Accounting
- System Performance
- PCI Compliance
- Packet Capture
- Auto Updates

Dashboard

Once the FortiConnect Setup Wizard has been completed the Dashboard will be the first thing an Administrator will see when they login to the network and can be reached by navigating to Home --> Dashboard

The screenshot displays the Meru Connect Administration interface. The top navigation bar includes the Meru logo, the title 'Meru Connect Administration', and user options: 'admin user', 'Logout', and 'About'. A sidebar on the left lists navigation items: HOME, Dashboard, My Settings, Setup Wizard, NETWORK ACCESS POLICY, POLICY SETTINGS, SPONSOR PORTAL, GUEST PORTALS, SMART CONNECT, DEVICES, REPORTS & LOGS, and SERVER.

The main dashboard area is divided into four sections:

- Critical Alerts & Messages:** A table with columns 'Message' and 'Date/Time'. It shows 'No Records Found' and a message: 'CPU usage is very high.' (indicated by a red dot).
- Guest Statistics:** A table showing user account statistics:

User Accounts	
Total:	0
Active:	0
Inactive:	0
Expired:	0
Suspended:	0
Rejected:	0
Pending Approval:	0
- System:** A table showing system status:

System	
CPU	
Number of CPUs:	1
Usage:	High
Load Average:	
Last minute:	20.46
Last 5 minutes:	12.39
Last 15 minutes:	5.33
Memory and Disk	
Total server memory:	1.0GB
Total disk space:	35.4GB
Free disk space:	32.0GB
NTP (Time Synchronization)	
Status:	Stopped
Replication	
Enabled:	No
Service:	Stopped
- Application Logs:** A table with columns 'Sponsor/Admin User', 'Action', and 'Date/Time'. It lists recent events such as 'Login successful [admin]', 'Configuration settings saved', and 'Client network configuration [Client Access] saved'.

At the bottom left, a copyright notice reads: '© 2011-2014 Meru Networks. All rights reserved.'

There are 4 sections this dashboard contains as follows:

1. Critical Alerts & Messages
2. Guest Statistics
3. System
4. Application Logs

Critical Alerts & Messages

This section refreshes itself automatically every minute to display the latest data and also shows the 10 latest critical alerts.

It will also show the following messages as and when the conditions are met :

- Packet capture is running
- The server has less than 1GB of memory

- The total disc spaces is less than 20GB
- The free disc space is less than 1GB
- RADIUS is running in debug mode
- No response from the DNS server
- License is going to expire within 30 days
- Have set detailed log level in Log Settings
- Replication is on but service is stopped
- CPU usage is high

Guest Statistics

This sections refreshes itself automatically after 67 seconds to display the latest data on the number of different users with different statuses.

Statuses that will be displayed are as listed :

- Created
- Authenticated
- Connected
- Active
- Pending Approval
- Rejected
- Suspended
- Expired

It also shows the following in this section :

- License expiry date - It will detail whether the license installed on the system is a permanent license or if expiry remains is less than 61 days then the number of days remaining will be shown.
- Users limit - Number of times the limit has been exceeded in the last 7 days.

System

This section refreshes itself periodically to display the latest data on performance as follows :

- CPU usage
- Average CPU load in the last 1, 5 and 15 minutes

- Total system memory in GB
- Total disc space
- Free space available
- NTP status
- Replication status

Application Logs

This section does not refresh itself automatically but does contain a link to refresh once clicked and displays the most recent 100 application log entries into the system.

SNMP Configuration

FortiConnect supports management applications monitoring the system over SNMP (Simple Network Management Protocol). SNMP Versions 1, 2c and 3 are supported.

The appliance can also send SNMP traps and informs when certain settings exceed a defined value.

SNMP Agent Configuration

From the administration interface, select Server > SNMP as shown below.

SNMP Agent

Agent | Traps

SNMP Version 1

Enable V1: ☐

Read Community:

SNMP Version 2c

Enable V2c: ☐

Read Community:

SNMP Version 3

Enable V3: ☐

Username:

Password: Confirm:

Authentication Protocol:

Privacy Protocol:

Security Type:

Allowed IP Addresses

IP Range	
0.0.0.0/0	
<input type="text"/> / <input type="text"/>	<input type="button" value="Add"/>

You can configure the following options:

- Configuring SNMP Version 1
- Configuring SNMP Version 2c
- Configuring SNMP Version 3
- Configuring SNMP Allowed Addresses

Configuring SNMP Version 1

1. To enable SNMP Version 1, check the Enable V1 checkbox.
2. Enter an SNMP Read Community name to be used for read access.

3. Configure the Allowed IP Addresses allowed to access the appliance using SNMP by following the instructions in Configuring SNMP Allowed Addresses.
4. Click Save

Configuring SNMP Version 2c

1. To enable SNMP Version 2c, check the Enable V2c checkbox.
2. Enter an SNMP Read Community name to be used for read access.
3. Configure the Allowed IP Addresses allowed to access the appliance using SNMP by following the instructions in Configuring SNMP Allowed Addresses.
4. Click Save.

Configuring SNMP Version 3

1. To enable SNMP Version 3, check the Enable V3 checkbox.
2. Enter a Username to be used for read access.
3. Enter the Password and confirm it to make sure it has been entered correctly.
4. Select an Authentication Protocol from the dropdown menu: MD5 (HMAC-MD5-96) or SHA (HMAC-SHA-96).
5. Select a Privacy Protocol from the dropdown menu: DES or AES.
6. Select the Security Type to use from the dropdown menu: Authentication or Encryption.
7. Configure the Allowed IP Addresses allowed to access the appliance using SNMP by following the instructions in Configuring SNMP Allowed Addresses.
8. Click Save.

Configuring SNMP Allowed Addresses

1. Enter an IP Address Range made up of an IP Address and a prefix length. For example:
 - 0.0.0.0/0 to allow any address to access the appliance by SNMP.
 - 192.168.1.0/24 to allow any address from the 192.168.1.0-255 to access the appliance.
 - 172.16.45.2/32 to allow only the host 172.16.45.2 to access the appliance.

2. Click the Add button.
3. You can repeat Step 1 and Step 2 for as many addresses as you like.
4. Click Save.

Configuring SNMP Trap Support

The FortiConnect can be configured to send SNMP Traps to an SNMP Manager based upon certain system events.

Configuring SNMP Traps

1. From the administration interface, select Server > SNMP and click on the Traps tab as shown below.

SNMP Traps

Agent **Traps**

Traps

Enable Traps : ☒

Trap Version: Version 1

Community: public

Disk Space

Send trap if free disk space less than: 50% (currently 90% free)

Load Average

Send trap if Load Average goes above: 25 over one minute (currently 2.29)

Send trap if Load Average goes above: 10 over five minutes (currently 7.74)

Send trap if Load Average goes above: 5 over fifteen minutes (currently 4.65)

Send Traps To

IP Address	
	Add

Save Cancel

2. Check the Enable Traps checkbox if you want to enable traps.

3. Select the Trap Version from the dropdown: Version 1, Version 2c or Informs.
4. Enter the community string which will be validated by the receiving trap service.
5. The FortiConnect sends a trap if the disk space goes below a specified value. Enter the value you want the trap to be sent at in the Disk Space dropdown field.
6. Specify the Load Average that you want a trap to be sent if it exceeds the value over 1 minute, 5 minutes or 15 minutes. Load Average is calculated using the standard Linux formula and can be seen from the command line with the uptime command.
7. Enter each IP Address that you want to send a SNMP trap to and click the Add button.
8. Click the Save button to save the changes.

The following traps are sent :-

- a cold start trap is sent when SNMP traps are enabled or reconfigured
- a trap is sent when disk space falls below the percentage set in the UI
- a CPU load trap is sent if the load averages exceed those that are set in the UI
- when the server is low on temporary (swap) disk space
- support dskTable to give an simpler view of disk statistics.

Reports and Logging

System Logging

All actions within the FortiConnect are logged into the database. This enables you to:

- View any action that occurred as part of the normal operating process of the application
- Log administrator and sponsor actions
- Create system logs

Note: It is important to create and constantly maintain logging levels. Refer to Log Settings for details.

Audit Logs

Audit logs create a record of administrator and sponsor actions and can be created using four different methods.

1. To access the audit log functions from the administration interface, select Reports & Logs > System Logs as shown below and click the Audit Logs tab.

The screenshot displays the 'System Logs' interface. At the top, there is a blue header bar with the text 'System Logs'. Below this, there are four tabs: 'Audit Logs' (which is selected and highlighted in blue), 'Application Logs', 'Support Logs', and 'Log Settings'. The 'Audit Logs' tab contains several search filters: 'Action By:' with a text input field, 'Client IP:' with a text input field, and 'Server IP:' with a dropdown menu currently set to 'Show All'. Below these, there is a 'Between:' section with date pickers for '1', 'Dec', and '2014', followed by 'and:' and another set of date pickers for '2', 'Dec', and '2014'. At the bottom of the filter section, there are two buttons: 'Run' and 'Cancel'.

2. Audit log reports can be run using four different categories:
 - Action by—Displays logs using admin/sponsor user name as its search criteria.
 - Client IP—Displays logs using Client IP address as its search criteria.
 - Server IP—Displays logs using Server IP as its search criteria.

You can run log reports for a single category, multiple categories, or all categories at the same time.

3. Select a time duration for your search criteria using the date pickers provided, then click the Run button.

Application Logs

Application Logs shows the application log containing application debugs.

1. To access the Application Logs function from the administration interface, select Reports & Logs > System Logs and click the Application Logs tab as shown below.

System Logs

Audit Logs **Application Logs** Support Logs Log Settings

Action By: Client IP:

Between: 1 Dec 2014 and: 2 Dec 2014

Run Cancel

Sponsor/Admin User ▲▼	Action ▲▼	Date/Time ▲▼
admin	Login successful [admin]	02-Dec-2014 12:44:52
admin	Configuration settings saved	02-Dec-2014 12:28:12
admin	Test URL returned [6] [Could not resolve host: scep; Unknown error; URL: http://scep]	02-Dec-2014 12:21:54
admin	Login successful [admin]	02-Dec-2014 12:19:13
admin	Client language template (2) updated	02-Dec-2014 12:07:18
admin	Client Language template (Meru Template) added, with component values as Default template	02-Dec-2014 12:06:21
admin	Client network configuration [Client Access] saved	02-Dec-2014 11:50:15
admin	Client network configuration [Client Access] saved	02-Dec-2014 11:49:33
admin	Client network configuration [Client Access] saved	02-Dec-2014 11:48:39
admin	Client network configuration [Client Access] saved	02-Dec-2014 11:47:53

Showing 1-10 of 86 10 per page Go

Page 1 of 9 Go

2. Application Log reports can be run using different categories:
 - Action By—Displays logs using admin/sponsor user name as its search criteria.
 - Client IP—Displays logs using Client IP address as its search criteria.

You can run log reports for a single category, multiple categories, or all categories at the same time.

3. Select a time duration for your search criteria using the date pickers provided then click the Run button.

Support Logs

Support Logs provide an area that stores:

- HTTP error logs
 - RADIUS logs
 - Mail logs
 - Twin (Replication logs only applicable if running replication between FortiConnects)
 - Debug logs
 - Audit logs
 - Application logs
 - An XML file
1. To access the Support Logs function from the administration interface, select Reports & Logs > System Logs and click the Support Logs tab as shown below

The screenshot shows the 'System Logs' interface with the 'Support Logs' tab selected. A link 'Download support log bundle' is visible above a table of log files.

File	Size	Lines	Action
HTTP Error Log	4 870	56	View
HTTPS Error Log	888	8	View
RADIUS Log	97 283	1 229	View
RadSec log	1 206	18	View
Mail Log	1 968	21	View
System Messages	56 037	650	View
Application Log	1 133	11	View
Postgres Startup Log	1 264	33	View
Postgres Tuesday Log	2 145	30	View
pgbouncer	5 195	52	View
Cron Log	566 530	5 076	View

2. You can view or download the logs listed by clicking the underlined Action links.

Note: The Support Logs page only displays the latest details of each available log. However, clicking View or Download retrieves and displays ALL logs for that category.

Log Settings

The Log Settings page allows an administrator to set the level of logging and administer syslog settings.

1. To access the Log Settings page from the administration interface, select Reports & Logs > System Logs and click the Log Settings tab as shown below.

System Logs

Audit Logs Application Logs Support Logs **Log Settings**

Logging Levels

General: Errors and Notices Only

Sponsor Authentication: Errors and Notices Only

Admin Authentication: Errors and Notices Only

Account Creation: Errors and Notices Only

Account Management: Errors and Notices Only

Admin Operations: Errors and Notices Only

RADIUS User Authentication: Errors and Notices Only

Guest Portals: Errors and Notices Only

Syslog Settings

Send Application Log Events to Remote Server: (none)

Send System Log Events to Remote Server: (none)

Syslog Server:

Syslog Protocol: ☒ UDP ☐ TCP

Syslog Port: 514

Save Cancel

2. **Logging Levels** allow an administrator to choose the level of logging for multiple criteria:
 - **General**—Allows an administrator to set logging of Errors and Notices only, Errors Notices and Info, or Errors Notices Info and Debugs.
 - **Sponsor Authentication**—Allows an administrator to set logging of Errors and Notices only, Errors Notices and Info, or Errors Notices Info and Debugs.
 - **Admin Authentication**—Allows an administrator to set logging of Errors and Notices only, Errors Notices and Info, or Errors Notices Info and Debugs.
 - **Account Creation**—Allows an administrator to set logging of Errors and Notices only, Errors Notices and Info, or Errors Notices Info and Debugs.
 - **Account Management**—Allows an administrator to set logging of Errors and Notices only, Errors Notices and Info, or Errors Notices Info and Debugs.
 - **Admin Operations**—Allows an administrator to set logging of Errors and Notices only, Errors Notices and Info, or Errors Notices Info and Debugs.
 - **Radius User Authentication**—Allows an administrator to set logging of Errors and Notices only, Errors Notices and Info, or Errors Notices Info and Debugs.
 - **Guest Portals**—Allows an administrator to set logging of Errors and Notices only, Errors Notices and Info, or Errors Notices Info and Debugs.
3. **Syslog Settings** allows an administrator to determine what log events are sent to a predefined syslog server.
 - **Send Application Log Events to Remote Server**—This determines what type of application errors are logged and sent to the server. The administrator can decide on none, Audit, Errors or Audit and Errors.
 - **Send System Log Events to Remote Server**—This determines what type of system errors are logged and sent to the server. The administrator can decide on Emergency, Emergency and Alerts, Emergency Alerts and Critical, or Emergency Alerts Critical and Errors.
 - **Syslog Server**—Enter the DNS or IP Address of the syslog server to which the logs to be sent.
 - **Syslog Protocol**—Choose between UDP and TCP protocols.
 - **Syslog Port**—Define a port for your syslog server.
4. Click the **Save** button to save your settings.

Note: To test basic syslog functionality, go to the Log Settings page and click **Save**. This sends a test message to the syslog server with priority info (6).

Note: IdentityNetworks recommends disabling debugging immediately after use so as not to potentially disrupt any other FortiConnect functionality.

RADIUS Authentications

To run a report on successful or failed RADIUS Authentications, go to **Reports & Logs > System Logs**

and click on RADIUS Authentications as shown below.

RADIUS Authentications

Enable RADIUS Authentication reporting: ☒

Between: 2 Dec 2014 00:00

and: 3 Dec 2014 00:00

Username:

Client IP Address:

Client MAC Address:

NAS IP Address:

Status: Failed Authentications

Run

Username	Status	IP Address	MAC Address	Time	NAS IP Address
No Records Found					

- Choose your search criteria using the fields available :-
 - Between - Choose the start date and time for your search.
 - and - Choose the end date and time for your search.
 - Username - Enter the Username of the account you wish to search against.
 - Client IP Address - Enter the Client IP Address you wish to search against.
 - Client MAC Address - Enter the Client MAC Address you wish to search against.
 - NAS IP Address - Enter the NAS IP Address you wish to search against.
 - Status - From the drop down menu select whether you wish to search for Failed Authentications, Successful Authentications or All Authentications.
- Click on Run to start your report.

User Accounts

FortiConnect can also perform a detailed search on User Accounts

To run this report follow the instructions below.

1. To access the User Accounts reporting function from the administration interface, select Reports & Logs > User Accounts and click the Advanced Search tab as shown below

The screenshot shows the 'User Accounts' section of the FortiConnect administration interface. At the top, there is a blue header bar with the text 'User Accounts'. Below this, there is a search bar with the text 'Active Time Between 25-Nov-2014 And 02-Dec-2014' and a button labeled '<< Advanced Search'. The search form contains several input fields and checkboxes:

- Sponsor Group: All (dropdown menu)
- Active Time Between: 25 Nov 2014 (calendar icon)
- Created By: (text input)
- And: 2 Dec 2014 (calendar icon)
- Guest Portal: (text input)
- Timezone: All (dropdown menu)
- Username: (text input)
- IP Address: (text input)
- MAC Address: (text input)
- Usage Profile: (text input)
- First Name: (text input)
- Account Group: (text input)
- Last Name: (text input)
- Event Code: (text input)
- Company: (text input)
- Email: (text input)
- Mobile Number: (text input)
- Inactive: ☐
- Active: ☐
- Expired: ☐
- Suspended: ☐
- Pending Approval: ☐
- Rejected: ☐

Below the search form, there are five buttons: 'Display Report', 'Download PDF', 'Download Excel', 'Download ODS', and 'Download ODT'. At the bottom, there is a table with the following columns: 'Created By', 'Username', 'Password', 'MAC Address', 'First Name', 'Last Name', 'Email', and 'Company'. The table currently shows 'No Records Found'.

2. Using the search filters, enter any information relevant to your search.
 - Sponsor Group - Use the drop down menu to select which Sponsor Group you wish to search under.
 - Active Time Between - Enter a start and end time to search under.
 - Created By - Search using Created By as your search criteria.

- Guest Portal - Search using Guest Portal as your search criteria.
 - Username - Search using Username as your search criteria.
 - MAC Address - Search using MAC Address as your search criteria.
 - First Name - Search using First Name as your search criteria.
 - Last Name - Search using Last Name as your search criteria.
 - Company - Search using Company as your search criteria.
 - Mobile Number - Search using Mobile Number as your search criteria.
 - Timezone - Search using a specific Timezone as your search criteria.
 - IP Address - Search using IP Address as your search criteria.
 - Usage Profile - Search using Usage Profile as your search criteria.
 - Time Profile- Search using Time Profile as your search criteria.
 - Guest Role - Search using Guest Role as your search criteria.
 - Event Code - Search using Event Code as your search criteria.
 - Email - Search using Email as your search criteria.
3. Check the appropriate check box for the account status -
- Active
 - Inactive
 - Suspended
 - Rejected
 - Expired
 - Pending Approval
4. Now decide how you want your report format -
- Display Report - Display report on screen
 - Download PDF - Downloads report as a PDF file
 - Download Excel - Download report as an excel spreadsheet
 - Download ODS - Download report as an ODS file
 - Download ODT - Download report as an ODT file

RADIUS Accounting

FortiConnect can also perform a detailed search on RADIUS Accounting

1. To access the RADIUS Accounting reporting function from the administration interface, select Reports & Logs > RADIUS Accounting and click the Advanced Search button as shown below.

RADIUS Accounting

Between 25-Nov-2014 And 03-Dec-2014 << Advanced Search

Between: 25 Nov 2014 And: 2 Dec 2014

Username: NAS IP Address:

Calling Station ID: User IP Address:

Called Station ID:

Display Report Download PDF Download Excel Download ODS Download ODT

Username ▲▼	Session ID ▲▼	Unique ID ▲▼	NAS IP Address ▲▼	Framed IP ▲▼	Start Time ▲▼	Stop Time ▲▼
No Records Found						


2. Using the search filters, enter any information relevant to your search.
 - Between - Enter a start date for your search
 - and -Enter and end date for your search
 - Username - Enter a username to search against
 - Calling Station ID - Enter a calling station ID to search against
 - Called Station ID - Enter a called station ID to search against
 - NAS IP Address - Enter a NAS IP Address to search against
 - User IP Address - Enter a user IP address to search against
3. Now decide how you want your report format -
 - Display Report - Display report on screen
 - Download PDF - Downloads report as a PDF file
 - Download Excel - Download report as an excel spreadsheet
 - Download ODS - Download report as an ODS file
 - Download ODT - Download report as an ODT file

System Performance


FortiConnect Identity can also perform a detailed report on System Performance.

1. To access the System Performance reporting function from the administration interface, select Reports & Logs > System Performance as shown below.

System Performance

Between: 2 Dec 2014 

00 00

and: 3 Dec 2014 

00 00

Showing 1-25 of 57 25 per page <input type="button" value="Go"/>						
Time ▲▼	%user	%nice	%system	%iowait	%steal	%idle
02-Dec-2014 14:10	2.43	0.00	8.35	1.19	0.00	88.03
02-Dec-2014 14:00	1.14	0.00	8.38	1.02	0.00	89.47
02-Dec-2014 13:50	0.89	0.00	7.00	0.56	0.00	91.55
02-Dec-2014 13:40	1.03	0.00	7.56	0.57	0.00	90.83
02-Dec-2014 13:30	1.34	0.00	7.84	1.25	0.00	89.57
02-Dec-2014 13:20	1.26	0.00	7.52	0.57	0.00	90.65
02-Dec-2014 13:10	1.45	0.00	8.26	0.89	0.00	89.41
02-Dec-2014 13:00	1.23	0.00	9.44	0.88	0.00	88.45
02-Dec-2014 12:50	2.09	0.00	11.86	6.65	0.00	79.40
02-Dec-2014 12:40	0.88	0.00	7.44	0.76	0.00	90.91
02-Dec-2014 12:30	1.30	0.00	8.38	1.22	0.00	89.10
02-Dec-2014 12:20	1.28	0.00	7.66	1.02	0.00	90.04
02-Dec-2014 12:10	1.33	0.00	7.24	0.77	0.00	90.66
02-Dec-2014 12:00	1.30	0.00	7.06	0.50	0.00	91.14
02-Dec-2014 11:50	1.33	0.00	7.16	0.90	0.00	90.61
02-Dec-2014 11:40	1.13	0.00	6.94	0.52	0.00	91.40
02-Dec-2014 11:30	1.05	0.00	6.93	0.36	0.00	91.66
02-Dec-2014 11:20	1.29	0.00	7.17	0.62	0.00	90.92
02-Dec-2014 11:10	1.32	0.00	7.17	0.47	0.00	91.04
02-Dec-2014 11:00	1.86	0.00	9.31	0.76	0.00	88.07
02-Dec-2014 10:50	1.12	0.00	8.70	0.54	0.00	89.64
02-Dec-2014 10:40	1.61	0.00	7.81	0.87	0.00	89.71


- Using the Date Picker, select the relevant dates to search between and click on Run.
- Your report should appear below.
- Click on the Download CSV button to download the report in a CSV format,

PCI Compliance

This is a report to verify that all the settings required to be PCI 2.0 compliant are enabled.

It shows the status, and provides help/links to actions required to remediate any issues.

1. To access the System Performance reporting function from the administration interface, select Reports & Logs > PCI 2.0 Compliance as shown below.

PCI 2.0. Compliance Report			
 This report displays the current state of PCI 2.0 compliance for the existing IDM configuration.			
Showing 1-5 of 42 5 per page Go			
PCI DSS Requirement ▲ ▼	Component ▲ ▼	State	Details / Action
01. Maintain Firewall Configuration To Protect Cardholder Data	Open Port: 1812 & 1813	✓	Required by RADIUS service
01. Maintain Firewall Configuration To Protect Cardholder Data	Open Port: 1645 & 1646	✓	Required by RADIUS service
01. Maintain Firewall Configuration To Protect Cardholder Data	Open Port: 443 & 8443	✓	Required by web server for HTTPS traffic
01. Maintain Firewall Configuration To Protect Cardholder Data	Open Port: 22	✓	Required by secure shell (SSH)
01. Maintain Firewall Configuration To Protect Cardholder Data	Open Port: 31415	✓	Required by replication services
Page 1 of 9 Go			

2. Columns detailed in this report are :-

- PCI DSS Requirement - PCI requirement
- Component - Component effected
- State - A green tick shows this is captured, a red cross states that its required for compliance
- Details / Action - Details of requirement and any actions needed to make it compliant

Packet Capture

FortiConnect allows the admin user to record packet data from an IP address / network range for all network traffic or packets to specific ports.

The packet capture tool generates log files which can be downloaded & viewed using a packet viewing utility such as wireshark.

Only the last 10 generated capture logs are shown in the log table.

1. From the FortiConnect Administration Database browse to Server --> Packet Capture as shown below.

Packet Capture

Capture Settings

Network Range: / All Traffic: ☒

ICMP:

☐

UDP 1645 (RADIUS auth):

☐

TCP 80 (HTTP):

☐

UDP 1646 (RADIUS acct):

☐

TCP 8080 (HTTP):

☐

UDP 1812 (RADIUS auth):

☐

TCP 443 (HTTPS):

☐

UDP 1813 (RADIUS acct):

☐

TCP 8443 (HTTPS):

☐

UDP 3799 (RADIUS COA):

☐

TCP 389 (LDAP):

☐

TCP 22 (SSH / SCP / SFTP):

☐

TCP 636 (LDAPS):

☐

TCP 20 / 21 (FTP):

☐

TCP 88 (Kerberos):

☐

UDP 123 (NTP):

☐

UDP 88 (Kerberos):

☐

UDP 161 (SNMP):

☐

TCP 749 (Kerberos):

☐

UDP 162 (SNMP Traps):

☐

TCP 750 (Kerberos):

☐

UDP 53 (DNS):

☐

TCP 25 (SMTP):

☐

TCP 53 (DNS):

☐

TCP 31415 (Replication):

☐

Start

Stop

Capture Logs


The last 10 capture logs generated are shown.







File	Size (kb)
No log files found	

2. Enter the Network Range you wish to capture traffic to, or place a check in the All Traffic check box to capture all traffic.
3. If you do not wish to capture all traffic, you may place a check in the check boxes provided to capture the relevant traffic.

4. Click on the Start button.
5. Once the logs have been completed you will see them listed as per below.

Capture Logs

 The last 10 capture logs generated are shown.

File	Size (kb)	
2011-09-12T14:58:23-07:00.pcap	268.98	 
2011-09-12T14:58:04-07:00.pcap	178.34	 
2011-09-12T14:57:47-07:00.pcap	1.63	 

6. Download the logs by clicking on the download icon.
7. You can delete any logs by clicking on the bin icon.

Automatic Updates

As Smart Connect clients are updated and released more quickly than FortiConnect releases Automatic Updates is a feature used to update certain parts of FortiConnect to support those new clients.

Enable Automatic Updates to allow FortiConnect to securely download browser detection rules and Smart Connect updates.

This enables the system to identify the latest browser versions & client platforms without needing to update the main FortiConnect software.

Updates can be scheduled as a batch job to run on a daily, weekly or monthly basis at a given time.

Updates are retrieved from a cloud based CDN. Proxy settings (with / without basic authentication) can be used if needed for external network access.

1. From the FortiConnect Administration interface go to Server --> Automatic Updates as shown below.

Automatic Updates

Enable Automatic Updates to allow Meru Connect to securely download browser detection rules and Smart Connect updates. This enables the system to identify the latest browser versions & client platforms without needing to update the main Meru Connect software.

Enable Automatic Updates: ☒

Schedule

Frequency:

Day of the week:

Day of the month:

Time:

HTTP Proxy

Enable Proxy: ☒

Server:

Port:

Authentication:

Username:

Password: Confirm:

2. Check the Enable Automatic Updates check box to enable Automatic Updates.
3. In the Schedule section, use the drop down box to select :-
 - Frequency - Choose from Daily, Weekly or Monthly updates.
 - Day of the Week - Choose which day of the week you wish to perform your update.
 - Day of the Month - If you have chosen Monthly updates, select which day of the month you wish to perform the update.
 - Time - Choose the time of the day you wish to perform the update.
4. Check the Enable Proxy check box to enter your proxy server details.
5. In the Proxy section, use the fields to enter your proxy server information :-
 - Server - Enter your server hostname or IP address.
 - Port - Enter the port number for your proxy server.
 - Authentication - Use the drop down menu to select the method of authentication for the proxy server.

Automatic Updates

- Username - Supply the username used to authenticate against the proxy server.
- Password - Enter the password for the proxy server and confirm it.

6. Click on Save once you have made your selections.

Note: Click on the Update Now button to perform an immediate update.

Licensing

FortiConnect provides multiple Licensing options, the section below details how licensing works on your FortiConnect.

There are two kinds of license that are required for the FortiConnect Appliance

- Device License - This license is unique to a single FortiConnect Appliance (Hardware or Virtual Machine). The device license allows FortiConnect to run on the Appliance. You may install only a single Device License on an appliance.
- User Feature License - This license allows for concurrent usage on a per user basis. Multiple User Feature Licenses can be installed and they are additive.

Authenticated Users

Users are referred to as accounts that are either a person or a device and have been authenticated onto the network either internally, for example against the local FortiConnect database or with PMS (Property Management System) accounts, or externally by using AD, or a Social Media login.

FortiConnect allows the system to have the same amount of concurrent Users attached to the User network as user licenses.

There are no limits on the amount of authenticated accounts that can be created, only a connected User will consume a license.

How licenses are consumed

- Each connected User account (as recorded by RADIUS accounting) consumes a single User license.
- Each connected device account unrelated to a User account consumes a single User license.
- Multiple devices registered by a single User account consume a single User license.

Licensing

To view or upload a license from the administration interface:

1. Select Server > Licensing as shown below.

Licensing

System Information

Serial Number: VMware-56 4d b3 0c ac 5e ee 10-9c d3 f8 4f a6 de 56 f5
System ID: ce74-4745-a4d3-8fa7-a693-30df-6e91-0ca2-7344-9166

Licence Summary

For information on licensing go to <http://www.merunetworks.com/license>

Feature	Settings	Expiry
Meru Connect	Enabled	31-Jan-2015
Users	Concurrent Users: 100 / In Use: 0	31-Jan-2015

Upload new License

License File: No file chosen

Installed License Files

Features	Created	File
Meru Connect: Expiry: 31-Jan-2015 Users: 100	01-Dec-2014	

- Click the Choose File button under the Upload new License section and select the license file.
- Click the Upload button to upload a new license file.

If a license is currently installed the information will be displayed at the top of the page :

- Serial Number - Serial Number for the FortiConnect
 - System ID - System ID for the License granted.
- Under Licence Summary it displays -
 - Feature - Which feature of FortiConnect is being used.
 - Settings - Whether the feature is enabled and how many active licenses are in use.
 - Expiry - Expiry date of feature.

Note: If you have uploaded an evaluation license, the FortiConnect License Status will indicate the license expiration date.

5. Under Installed License Files, you have the ability to download licenses and delete license files if you have multiple license files installed.

Replication and Licensing on FortiConnect

When FortiConnects are replicated across a network, a license is installed on and shared between each system.

If one of the FortiConnect systems is disconnected from the network the remaining FortiConnect would continue to use the total license count of both systems. When connectivity is restored license sharing will resume automatically.

Sponsor Documentation

This chapter provides user documentation for sponsor users who create UserUser accounts. It contains the following sections:

- Introduction to FortiConnect
- Connecting to the FortiConnect
- Change Default Settings
- Guest User Accounts
- Multiple Guest Accounts
- Event Codes
- Reporting on Guest Users
- Device Accounts
- Multiple Device Accounts
- Sponsor Reporting

Introduction to FortiConnect

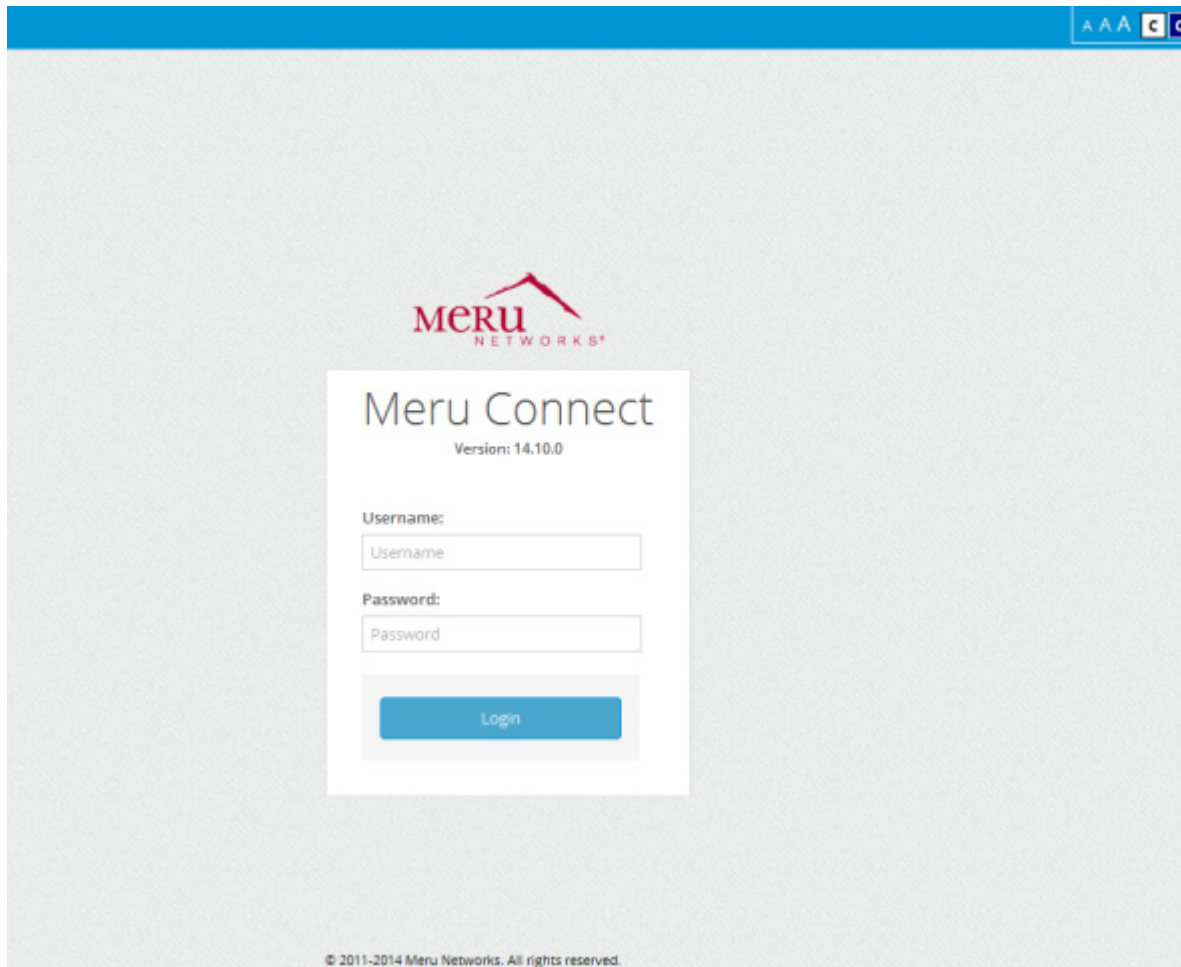
The FortiConnect allows you to create temporary network access accounts for your Users, visitors, contractors or anyone who needs temporary network access. You can easily create User or device accounts by browsing to the FortiConnect web interface, logging in with your corporate credentials, and entering the details of the User or device. FortiConnect creates the temporary account and allows you to provide the account details to the User via printout, email or SMS text message. In addition to creating User and device accounts, you can also view and amend the accounts to which you have access, or run reporting on accounts for auditing purposes.

Connecting to the FortiConnect

All connections to the FortiConnect are through a web interface. To connect to the FortiConnect, open a web browser and enter the address into the URL or address field, as provided by your network administrator.

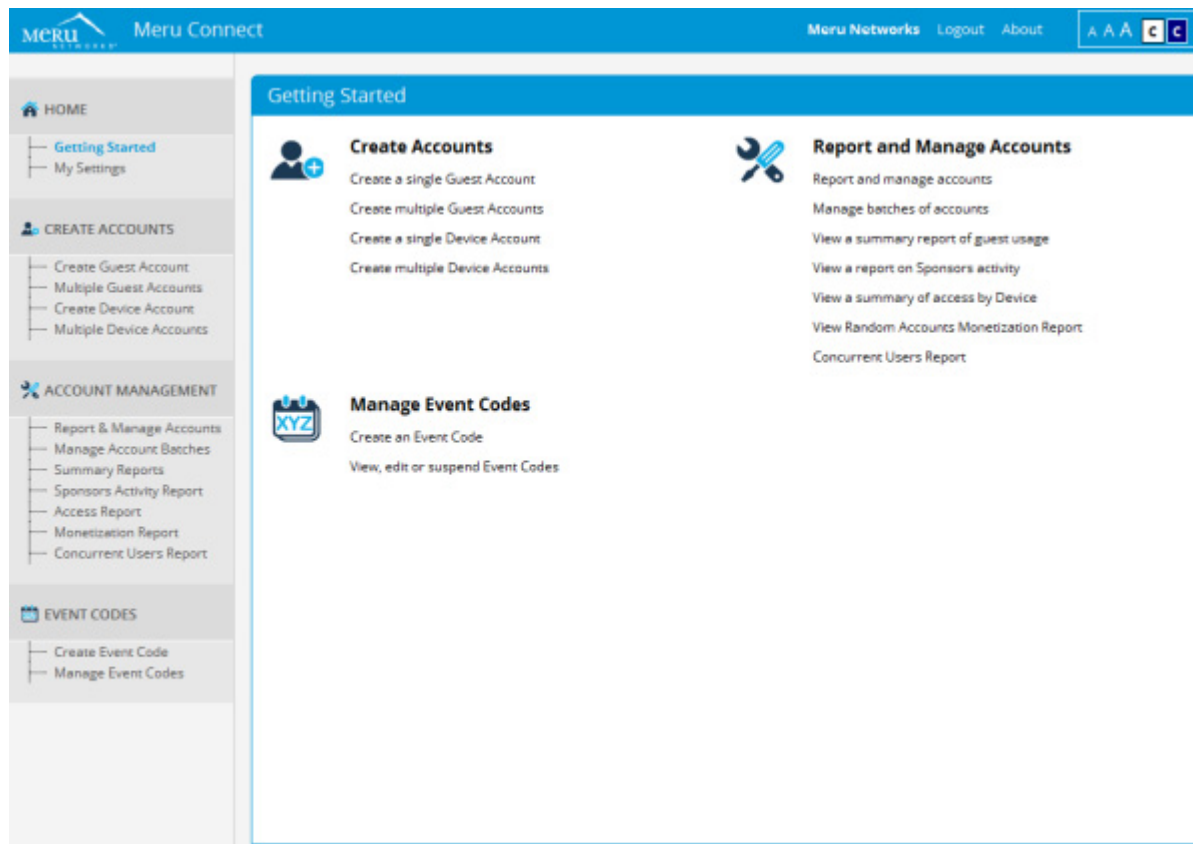
Connecting to the FortiConnect

1. Enter the IP address of the FortiConnect into the URL of your web browser, for example, `http://<IP Address of FortiConnect>`.
2. In the FortiConnect login page below, enter your Username and Password, and click the Login button. Use the login credentials specified by your network administrator.



The image shows the Meru Connect login page. At the top, there is a blue header bar with the text "AAA" and a small icon. Below the header, the Meru Networks logo is centered. The main content area is a white box with the title "Meru Connect" and "Version: 14.10.0". Below the title, there are two input fields: "Username:" and "Password:". Below the password field is a blue "Login" button. At the bottom of the page, there is a copyright notice: "© 2011-2014 Meru Networks. All rights reserved."

3. When you first log in, the Getting Started page is displayed as shown in below.



4. From this page, you can navigate to Home > My Settings to:

- Change Default Settings.
- Change Password.

Change Default Settings

You can change your password, or customize default settings like the language template, time zone, telephone country code, and default login page from the My Settings page.

1. Navigate to Home > My Settings
2. Click the Preferences tab as shown below, to modify the following Preferences:
 - **Language Template**—If your administrator has added additional templates, you can select a language template from this dropdown menu to change the language of the application interface or the User printout/email/SMS notification.
 - **Default Timezone**—This timezone is the default selected in the list on the account creation pages.

Change Default Settings

- Default Telephone Country Code—Specify the default for the telephone country code.
- This is used when sending the User details by SMS, or for recording the User's phone number.
- Default Guest Role—Specify the default User role you want to use for creating accounts.
- Default Device Role - Specify the default device role you want to use for creating accounts.
- First Name - Sponsors first name
- Last Name - Sponsors last name
- Email Address—Enter your email address here. This is required if you want to receive a copy of the User's account details by email.
- Receive Email Confirmation—Check this checkbox if you want the FortiConnect to send you a copy of the User's account details by email, when you click the 'Send Email Notification' button to notify the users of their User account details.
- Default Login Page—Using the dropdown menu, select the page that you want the FortiConnect to display immediately after you login.
- Use High Contrast UI - Click the check box to use a high contrast user interface.
- Base Font Size - From the drop down menu choose between Normal, Bigger or Biggest for a choice of font sizes.

The screenshot shows the 'My Settings' interface with the 'Preferences' tab selected. The settings are as follows:

Setting	Value
Language Template:	English (Default)
Default Timezone:	America/Los_Angeles
Default Telephone Country Code:	+1
Default User Group:	Default Account Group
Default Device Group:	Default Account Group
First Name:	Meru
Last Name:	Networks
Email Address:	merunetworks@meru.com
Receive Email Confirmation:	<input type="checkbox"/>
Default Login Page:	Getting Started
Use High Contrast UI:	<input type="checkbox"/>
Base Font Size:	Normal

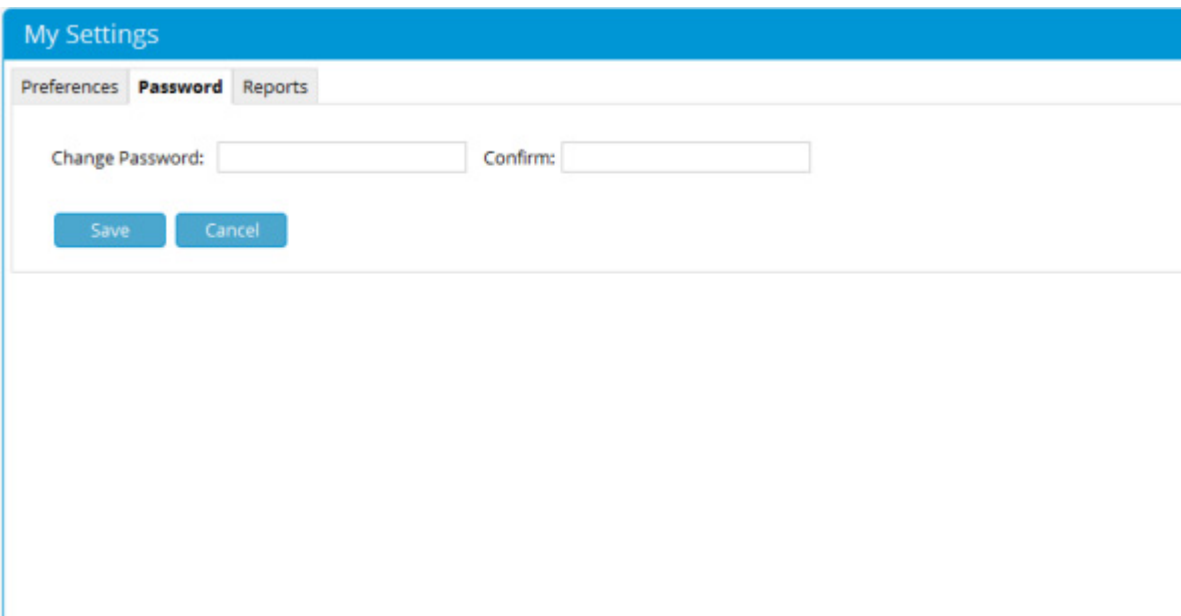
At the bottom of the form are two buttons: 'Save' and 'Cancel'.

3. Click the Save button to save your default settings.

Change Password

The Change Password option is enabled if your account is locally defined on the FortiConnect by your administrator. If you authenticated with a username/password from an external server such as Active Directory, you cannot view this option.

1. Navigate to Home > My Settings.
2. Click the Password tab as shown below.



The screenshot shows the 'My Settings' interface with a blue header bar. Below the header, there are three tabs: 'Preferences', 'Password' (which is selected and highlighted in blue), and 'Reports'. The 'Password' tab contains two input fields labeled 'Change Password:' and 'Confirm:'. Below these fields are two buttons: 'Save' and 'Cancel'.

3. Enter your new password in the Change Password and Confirm fields.
4. Click the Save button to save your new password.

Report Settings

You can select and deselect options you want to view in the Manage Accounts page or when exporting details from the Manage Accounts page.

1. Navigate to Home > My Settings

2. Click the Reports tab as shown below.

My Settings

Preferences

Password

Reports

	Report	Download
Created By:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Username:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
MAC Address:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Password:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
First Name:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Last Name:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Email:	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Company:	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Status:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Mobile Phone Number:	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Start Time:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
End Time:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Timezone:	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Account Group:	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Usage Profile:	<input type="checkbox"/>	<input checked="" type="checkbox"/>
option1:	<input type="checkbox"/>	<input checked="" type="checkbox"/>
option2:	<input type="checkbox"/>	<input checked="" type="checkbox"/>
option3:	<input type="checkbox"/>	<input checked="" type="checkbox"/>
option4:	<input type="checkbox"/>	<input checked="" type="checkbox"/>
option5:	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Event Code:	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Time Remaining:	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Price:	<input type="checkbox"/>	<input type="checkbox"/>

Save

Cancel

3. Check or uncheck the check boxes based on the options to be displayed in the Manage Accounts page on downloading a report.
4. Click the Save button when finished.

Creating Guest User Accounts

If you are assigned the appropriate permissions, you can create temporary user accounts.

1. Log into the FortiConnect as described in [Connecting to the FortiConnect](#).
2. Navigate to **Create Accounts > Create Guest Account**.
3. The Create Guest Account page appears as shown below.

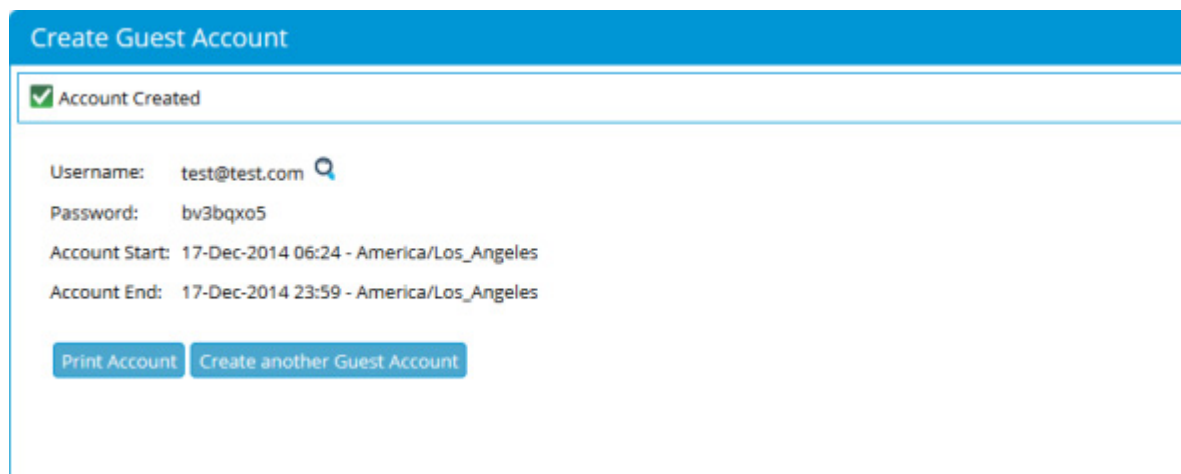
Note: The screenshot below shows the default template for creating a Guest User Account. Your administrator has the option to add or remove other fields.

The screenshot shows the 'Create Guest Account' form with the following fields and values:

- First Name:** [Empty text box]
- Last Name:** [Empty text box]
- Company:** [Empty text box]
- Email Address:** [Empty text box]
- Mobile Phone Number:** +1 [Empty text box]
- Timezone:** America/Los_Angeles [Dropdown menu]
- Account Start:** 2 Dec 2014 14:28 [Date and time pickers]
- Account End:** 2 Dec 2014 23:59 [Date and time pickers]
- Buttons:** Add User, Cancel

4. Enter the First Name of your User. Enter the Last Name of your User.
5. Enter the Company or organization of your User. Enter the Email Address of your User.
6. Enter the Mobile Phone Number of your User.
7. Select the Profile from the dropdown menu. This dropdown appears automatically if your administrator has defined Usage Profiles and more than one profile is available.
8. Choose the Timezone relevant to the time and date.

9. From the Account Start field, choose the Time and Date from which you want the account to be valid.
10. From the Account End field, choose the Time and Date at which you want the account to end.
11. If the administrator for FortiConnect has configured any additional required account attributes, specify the appropriate information for those settings in this form.
12. Click the Add User button. The account is created and the details are displayed as shown below.



The screenshot shows a web interface titled "Create Guest Account". At the top, there is a blue header bar with the title. Below the header, a green checkmark icon is followed by the text "Account Created". The main content area displays the following details:

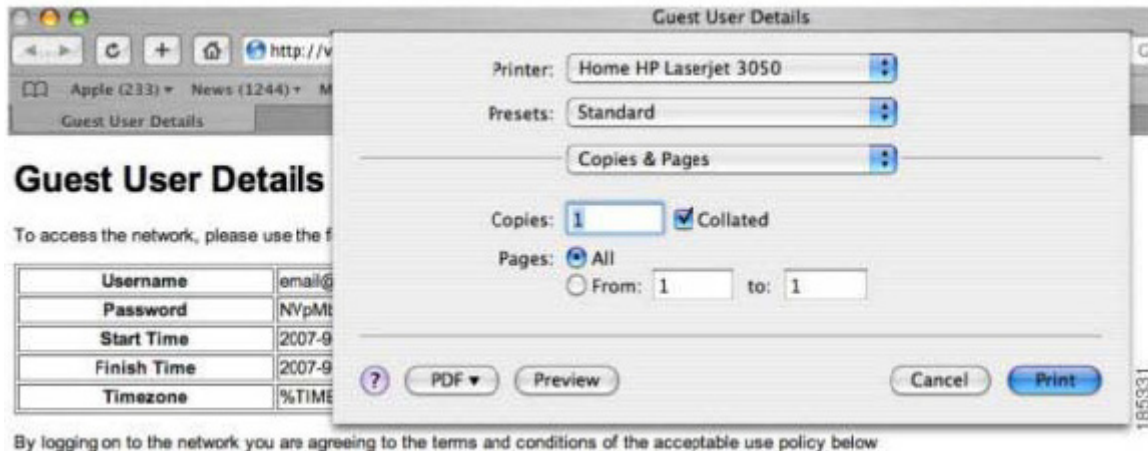
- Username: test@test.com (with a magnifying glass icon)
- Password: bv3bqxo5
- Account Start: 17-Dec-2014 06:24 - America/Los_Angeles
- Account End: 17-Dec-2014 23:59 - America/Los_Angeles

At the bottom of the form, there are two buttons: "Print Account" and "Create another Guest Account".

13. Depending on your permissions, you can perform one or all of the following actions on the same page where the new account details are displayed:
 - Clicking the Print Account button allows you to print the account details to your printer to hand to the User. These details commonly include User access instructions and usage policies. See Print Account Details.
 - Clicking the Email Account button sends the account details to the email address you entered for the User. See Email Account Details.
 - Clicking the Send SMS Message button sends the account details to the User's mobile phone via SMS text message. See Text Message Account Details (SMS).
14. You can also create another account immediately by clicking the Create another Guest account button.

Print Account Details

1. Click the Print Account button from the Create Guest Account page shown below.



2. A new Printer window opens and you can print out the user details.

Note: After a User account is created, you can also access this feature by navigating to Account Management > Manage Guests. Find the required User account from the list displayed, then click on the printer icon, labelled print account details, adjacent to the User account on the far right of the screen

Email Account Details

1. Click the Email Account button from the Create Guest Account page.
2. The FortiConnect sends an email to the email address specified when you created the account.

Note: After a User account is created, you can also access this feature by navigating to Account Management > Manage Guests. Find the required User account from the list displayed, then click on the envelope icon, labelled e-mail account details, adjacent to the User account on the far right of the screen.

Text Message Account Details (SMS)

1. Click the Send SMS Message button from the Create Guest Account page.
2. The FortiConnect sends a text message to the phone number specified in the account creation.

Note: After a User account is created, you can also access this feature by navigating to Account Management > Manage Guests. Find the required User account from the list displayed, then click on the mobile phone icon, labelled Send SMS Message, adjacent to the User account on the far right of the screen.

Multiple Guest Accounts

The FortiConnect allows you to create multiple accounts at the same time. The options available to you are configured by your administrator. They include:

- Creating Multiple Accounts from Text Entry
- Creating Multiple Accounts from CSV File
- Creating Multiple Random Accounts

You can create multiple accounts by pasting the details into the interface, importing a Comma Separated Values (CSV) file, or creating random accounts to be assigned to users (with the details recorded on paper) for input at a later time.

Creating Multiple Guest Accounts from Text Entry

1. Navigate to Create Accounts > Multiple Guest Accounts and click on the Multiple Guest Accounts tab as shown below.

Multiple Guest Accounts

Random Guest Accounts

Choose File No file chosen Import Download Template

	First Name	Last Name	Company	Country Code	Mobile Phone Number	Email Address
				+1 ▾		

Timezone:

America/Los_Angeles ▾

Account Start:

2 ▾

Dec ▾

2014 ▾

14 ▾

33 ▾

Account End:

2 ▾

Dec ▾

2014 ▾

23 ▾

59 ▾

Create Accounts Cancel

2. Enter the details in the grid fields as required with a cell separating the values.
 3. Select the Usage Profiles from the dropdown menu. This dropdown appears automatically if your administrator has defined Usage Profiles and more than one profile is available.
 4. Select the relevant Timezone for the account.
 5. Choose the Account Start time, and then the Account End time.
 6. Click the Create Accounts button.
- In the username and password fields, enter the username and the password for the User account you wish to create.

Creating Multiple Guest Accounts from CSV File

1. Navigate to **Create Accounts > Multiple Guest Accounts** and click on the **Multiple Guest Accounts** tab as shown below.

[illegible]

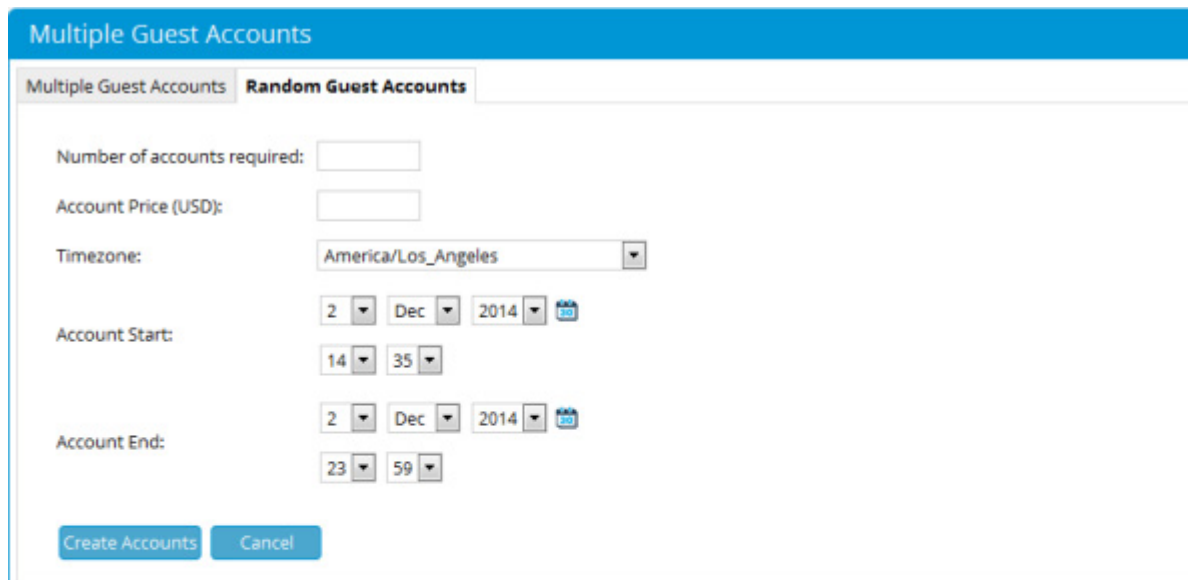
2. Download the CSV file by clicking the Download Template link and save this file locally.
3. Fill out the fields in the CSV Template file using a program such as Microsoft Excel:
 - First Name - The User's first name.
 - Last Name - The User's last name
 - Company - The User's company
 - Email Address - The User's email address
 - Country Code - The country code of the mobile phone number, for example 1 for the US, 44 for the UK.
 - Mobile Phone Number - The User's mobile phone number.
 - Note - Do not enter hyphens in the number.
 - Other details - Other details may be configured by your administrator and the names and descriptions are decided by them.
4. Save the CSV Template file in CSV format.
5. Click the Browse button to select your edited CSV file.
6. Select the Profile from the dropdown menu. This dropdown appears automatically if your administrator has defined Usage Profiles and more than one profile is available.

7. Select the relevant Timezone for the account.
8. Choose the Account Start time, and then the Account End time.
9. Click the Import button.

Creating Multiple Random Guest Accounts

You can create random accounts when you need to hand out details to visitors, but do not have access to a computer at the time you need to create and provide the accounts to Users. This feature allows you to create accounts in advance and record the details on paper, and store them in the system for correlation at a later time.

1. Navigate to Create Accounts > Multiple Guest Accounts as shown below. and click on the Random Guest Accounts Tab.























The screenshot shows a web interface titled "Multiple Guest Accounts". It has two tabs: "Multiple Guest Accounts" and "Random Guest Accounts", with the latter being selected. The form contains the following fields and controls:

- Number of accounts required:** A text input field.
- Account Price (USD):** A text input field.
- Timezone:** A dropdown menu currently showing "America/Los_Angeles".
- Account Start:** A date and time selector with dropdowns for day (2), month (Dec), and year (2014), followed by a calendar icon. Below it are dropdowns for hour (14) and minute (35).
- Account End:** A date and time selector with dropdowns for day (2), month (Dec), and year (2014), followed by a calendar icon. Below it are dropdowns for hour (23) and minute (59).
- Buttons:** "Create Accounts" and "Cancel" buttons at the bottom left.

2. Enter the number of accounts that you want to generate.
3. Select the Profile from the dropdown menu. This dropdown appears automatically if your administrator has defined Usage Profiles and more than one profile is available.

4. Select the relevant Timezone for the account.
5. Choose the Account Start time, and then the Account End time.
6. Click the Submit button. The random accounts are created and displayed as shown below.

Multiple Account Details								
Print All Download CSV		Showing 1-10 of 50 10 per page Go						
Username ▲▼	Password ▲▼	MAC Address ▲▼	First Name ▲▼	Last Name ▲▼	Status ▲▼	Start Time ▲▼	End Time ▲▼	
2k02HJgu	k8vxft5l				Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	 
2Wj8NooZ	y59sidhb				Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	 
3lxQaLfw	v49qzxoq				Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	 
3WYvM6xf	l4wni9fn				Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	 
52LtvVdo	j5wuqjd4				Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	 
5K8vF2h	wo3fbv7k				Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	 
6cy0DpsV	j1mun57y				Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	 
6FFff4r	qx8wkBoc				Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	 
6UQ7jkWp	xyme0bx8				Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	 
7QNaclH8	y6idt6ye				Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	 
Page 1 of 5 Go								

Printing/Email/SMS Multiple Guest Accounts

When you have created accounts using one of the multiple account creation methods, the screen for the users details is slightly different than the one shown when a single User account is created. You can Email and SMS all accounts to each individual User after creation. You can also print the details for each individual account, or download the accounts file in CSV format.

1. Navigate to Account Management > Manage Account Batches as shown below.

Manage Account Batches

Username:

MAC Address:

Showing 1-1 of 1

10 per page

Go

Batch ▲▼	Created By ▲▼	Created ▲▼	Accounts ▲▼	Total Value ▲▼
1417559865	meru networks	02-Dec-2014 14:37	50	500.00 (USD)































Page 1 of 1

Go

- Determine the batch of accounts you have created by the Time/Date Created column or by checking the Created By column. Click the bulk account ID link you have created to view the Multiple Account Details page as shown below.

3. When creating account batches, both for user and device accounts, the sponsor will be required to enter the batch name to place the accounts. If the sponsor specifies the name of an existing batch, the accounts will be added to that batch, if the sponsor specifies a new name, a new batch will be created with the accounts.

[illegible]

Multiple Account Details								
Print All Suspend All Download CSV								
Showing 1-10 of 50 10 per page Go								
Username ▲▼	Password ▲▼	MAC Address ▲▼	First Name ▲▼	Last Name ▲▼	Status ▲▼	Start Time ▲▼	End Time ▲▼	
2k0PhUqu	k@vxiff5l				Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	  
2Wj8NooZ	y59sidhb				Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	  
3lcQaL6w	v49qzxoq				Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	  
3WyyM6Xf	l4wni9fn				Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	  
52LtvVdo	j5wuqjd4				Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	  
5K8vF2h	wo3fbv7k				Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	  
6cY0DgsV	jlmun57y				Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	  
6FFiff4r	qx8wk8oc				Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	  
6UQ7jkWp	xyme6bx8				Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	  
7QNdnhH8	y6idt6ye				Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	  
Page 1 of 5 Go								

4. From this page you can:

- **Print All** –Click to print out the account details created for each User.
- **Email All** –Click to email the account details created to each User.
- **SMS All** –Click to SMS the account details created to all User.
- **Suspend All** –Click to suspend all the bulk accounts you have created.
- **Download CSV**–Click to download a CSV file of the bulk accounts created.
- **Suspend an account**–Click the hazard icon.
- **Edit an account**–Click the pencil icon to edit the individual account selected.
- **View an account in detail**–Click the notepad icon to view the individual account details.
- **Print account details**–Click the printer icon to print the individual account details.

Note: When creating accounts with preset details (by either importing text or creating a CSV file), you can print, email, or transmit via SMS the User account details. However, when you create random accounts, you can only use the print option.

Viewing Multiple Account Groups





















When creating bulk accounts, you can view batches of accounts that were created at the same time using one of the following three methods:

- Viewing Multiple Account Groups
- Finding Multiple Account Groups by Username
- Finding Multiple Account Groups on the Active Accounts Report

Viewing Multiple Account Groups


This option allows you to select the batch of accounts that you created.

1. Navigate to Account Management > Manage Account Batches.
2. Click the underlined link of the Bulk account ID you have created to bring up the Multiple Account Details.

Multiple Account Details								
Print All Suspend All Download CSV								
Showing 1-10 of 50 10 per page Go								
Username ▲▼	Password ▲▼	MAC Address ▲▼	First Name ▲▼	Last Name ▲▼	Status ▲▼	Start Time ▲▼	End Time ▲▼	
2k0PHUgu	k8vxff5l				Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	 
2Wj8NxxZ	y59sidhb				Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	 
3lcQal6w	v49qzxoq				Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	 
3WyyM6xf	l4wnl9fn				Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	 
52LtvVdo	j5wuqjd4				Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	 
5K8vEIZh	wo3fbv7k				Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	 
6cY00gkV	jimun57y				Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	 
6FFiff4r	qx8wk8oc				Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	 
6UQ7jkWp	xyme6bx8				Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	 
7ONadnH8	y6idt6ye				Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	 

- Click the underlined link of the account ID you have created to bring up the account details as shown below

Guest Account Details

Username:	6cY0DgKV 
Password:	jimun57y
Status:	Active
Account Start:	02-Dec-2014 14:35 - America/Los_Angeles
Account End:	02-Dec-2014 23:59 - America/Los_Angeles
First Name:	Not available
Last Name:	Not available
Company:	Not available
Email Address:	Not available
Mobile Phone Number:	Not available
Usage Profile:	default
Account Group:	Default Account Group
Account Price (USD)	10.00

[Print Account](#) [Suspend](#) [Reset Password](#)

Finding Multiple Account Groups by Username

This option allows you to find the batch of accounts by entering one username of the batch.



















1. Navigate to Account Management > Manage Account Batches.
2. Enter a username that belongs to a batch of accounts in the Username field and click the Submit button.

If found, the batch of accounts, that were created in the same operation as the username submitted, is displayed.

Finding Bulk Account Groups on the Active Accounts Report

This option allows you to find the batch of accounts from the Active Accounts Report page.

1. Navigate to Account Management > Manage Account Batches.
2. Click the underlined link of the Bulk account ID you have created to go to the Manage Accounts page for the bulk-created accounts. You can edit individual accounts in this page by clicking on the pencil icon next to the account you wish to edit.

Multiple Account Details								
Print All Suspend All Download CSV								
Showing 1-10 of 50 10 per page Go								
Username ▲▼	Password ▲▼	MAC Address ▲▼	First Name ▲▼	Last Name ▲▼	Status ▲▼	Start Time ▲▼	End Time ▲▼	
2k0PHUqu	k8vxff5l				Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	 
2Wj8NxxZ	y59sidhb				Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	 
3loQaL6w	v49qzxoq				Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	 
3WyyM6xf	l4wnl9fn				Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	 
52LtvVdo	j5wuqjd4				Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	 
5K8vEIZh	wo3fbv7k				Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	 
6cY00gkV	jimun57y				Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	 
6FFiff4r	qx8wk8oc				Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	 
6UQ7jkWp	xyme6bx8				Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	 

Managing Guest Accounts

You can view all accounts that have been created at any time using the Manage Guests page.































1. From the Main page select Account Management > Report and Manage Accounts.
2. On the Manage Accounts page, you can view the list of accounts that have been created as shown below. The fields displayed on this page can be customized using Report Settings.

Report & Manage Accounts

Created By: meru Status: Inactive,Active,Pending Approval: Active Time between 02-Nov-2014 01:00 and 02-Jan-2015 00:00 [Advanced Search >>](#)

[Run](#) [Save as Default](#) [Reset to Default](#) [Download CSV](#)

Showing 1-10 of 51 10 per page Go

<input type="checkbox"/>	Created By ▲▼	Username ▲▼	MAC Address ▲▼	Password ▲▼	First Name ▲▼	Last Name ▲▼	Status ▲▼	Start Time ▲▼	End Time ▲▼	
<input type="checkbox"/>	meru networks	meru@meru.com		5aj8gahg	User	One	Active	02-Dec-2014 14:28 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	  
<input type="checkbox"/>	meru networks	BjCGQNH7		tm9wpm6			Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	  
<input type="checkbox"/>	meru networks	nx3Z9Qet		ggk2ra3b			Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	  
<input type="checkbox"/>	meru networks	r9PYU3r4		jk6vrl3t			Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	  
<input type="checkbox"/>	meru networks	Eopk23ef		9exl5lci			Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	  
<input type="checkbox"/>	meru networks	5x8vF12h		wo3fbv7k			Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	  
<input type="checkbox"/>	meru networks	y5Xa9Q1f		zq3prwo3			Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	  
<input type="checkbox"/>	meru networks	K1m49mJ		9lbulu4d			Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	  
<input type="checkbox"/>	meru networks	w7Tg7u4p		anllwo9b			Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	  
<input type="checkbox"/>	meru networks	6UO7JkWo		xyme6bx8			Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	  

Page 1 of 6 Go

Editing Guest Accounts

If you create an account for a User and you need to extend their account access, you can change the expiry date and time of the account.































1. From the Main page select Account Management > Report and Manage Accounts.
2. In the Manage Guests page you can view a list of the accounts that you can edit as shown below.

Report & Manage Accounts

Created By: meru networks; Status: Inactive,Active,Pending Approval; Active Time between 02-Nov-2014 01:00 and 02-Jan-2015 00:00 [Advanced Search >>](#)

[Run](#) [Save as Default](#) [Reset to Default](#) [Download CSV](#)

Showing 1-10 of 51 10 per page [Go](#)

<input type="checkbox"/>	Created By ▲▼	Username ▲▼	MAC Address ▲▼	Password ▲▼	First Name ▲▼	Last Name ▲▼	Status ▲▼	Start Time ▲▼	End Time ▲▼	
<input checked="" type="checkbox"/>	meru networks	meru@meru.com		Saj@gehg	User	One	Active	02-Dec-2014 14:28 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	  
<input type="checkbox"/>	meru networks	BjCG0NH7		tmf9wpm6			Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	  
<input type="checkbox"/>	meru networks	ox329Qet		ggk2ra3b			Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	  
<input type="checkbox"/>	meru networks	rPPYU3r6		jk8vr3t			Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	  
<input type="checkbox"/>	meru networks	Eqpk23ef		9xv5lci			Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	  
<input type="checkbox"/>	meru networks	2K8vFjZh		wo3fbv7k			Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	  
<input type="checkbox"/>	meru networks	y5Xe9Q7f		zq3prwo3			Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	  
<input type="checkbox"/>	meru networks	KJm89mU		9lbulu4d			Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	  
<input type="checkbox"/>	meru networks	w7Tg2u8p		ani8wo9b			Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	  
<input type="checkbox"/>	meru networks	6UQ7Jk0yp		xyme6bx8			Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	  

[Suspend All](#)

Page 1 of 6 [Go](#)

- Click the pencil icon next to the account you want to change to go to the Edit User Accounts page Guest Self Service as shown below.

Edit User Account

Username: meru@meru.com

First Name:

Last Name:

Company:

Email Address:

Mobile Phone Number:

Re-apply usage profile:

4. Change the Account details.
5. Click the Save Changes button to update the account with the new details.

AP Usage Summary

Shows total unique users, total usage time and sessions count based on AP Name and NAS IP Address. From the main page select Account Management > AP Usage Summary to bring up the AP Usage Summary report page as shown below.

AP Usage Summary

View Between: 11 Jan 2015

And: 12 Oct 2015

Run

Showing 1-1 of 1 10 per page Go

AP Name ▲▼	NAS IP Address ▲▼	Total Unique Users ▲▼	Total Usage Time ▲▼	Sessions Count ▲▼
AP 25	172.19.41.240	12	1 hour(s), 42 minute(s)	23

Page 1 of 1 Go

User Activity Report

Shows total usage time, sessions count for each User based on AP Name, AP ID and NAS IP Address. From the main page select Account Management >User Activity Report to bring up the User Activity Report page as shown below.

Fortinet

Meru Connect

sp11 Logou

HOME

Getting Started

My Settings

CREATE ACCOUNTS

Create Guest Account

Multiple Guest Accounts

ACCOUNT MANAGEMENT

Report & Manage Accounts

Manage Account Batches

Summary Reports

Sponsors Activity Report

Access Report

Monetization Report

Concurrent Users Report

AP Usage Summary

User Activity Report

EVENT CODES

User Activity Report

View Between: 7 Oct 2015

And: 12 Oct 2015

NAS IP Address: All

AP Id: All

AP Name: All

Additional Filters: Username

Run

Showing 1-10 of 1010 per pageGo

Username	Total Usage Time	Sessions Count	NAS IP Address	AP Id	AP Name
AVON_1023_513	4.00 second(s)	1	172.19.41.240	25	AP-25
suma_manager@idmqa.com	6.00 second(s)	1	172.19.41.240	25	AP-25
sree1@idmqa.com	8.00 second(s)	2	172.19.41.240	25	AP-25
p2@test.com	10.00 second(s)	1	172.19.41.240	25	AP-25
user1@radius	14.00 second(s)	1	172.19.41.240	25	AP-25

Advanced Search

1. If your Account Management page returns a large number of users, you can perform an advanced search by clicking the Advanced Search button as shown below.

Report & Manage Accounts

Created By: meru networks; Status: Inactive,Active,Pending Approval; Active Time between 02-Nov-2014 00:00 and 02-Jan-2015 00:00 << Advanced Search

Sponsor Group:	All	Active Time Between:	2 Nov 2014
Created By:	meru networks		00 00
Guest Portal:		And:	2 Jan 2015
Username:			00 00
MAC Address:		Timezone:	All
First Name:		IP Address:	
Last Name:		Usage Profile:	
Company:		Account Group:	
Email:		Event Code:	
Mobile Phone Number:			
Inactive:	<input checked="" type="checkbox"/>		
Active:	<input checked="" type="checkbox"/>		
Expired:	<input type="checkbox"/>		
Suspended:	<input type="checkbox"/>		
Pending Approval:	<input checked="" type="checkbox"/>		
Rejected:	<input type="checkbox"/>		

Run Save as Default Reset to Default Download CSV

2. In the Advanced Search page that is displayed, you can enter the following criteria to make your search:

- Sponsor Group - From the drop down menu select a sponsor group to search in.
- Created by—Sponsor who created the account.
- Guest Portal - Search for a User on a specific portal they authenticated on.
- Username - Search for a User by their allocated username.
- MAC Address - Search using a specific MAC Address.
- First Name—First Name of User.
- Last Name—Last name of User.
- Company—Company or Organization of User.
- Email—Email address of User.
- Mobile Phone Number - Mobile number of User.
- Active Time Between—Start Time from which the search to start.
- And —End Time at which the search to end.
- Timezone—From the dropdown menu select a timezone to be searched.
- IP Address—IP Address of User workstation.
- Usage Profile - Search by Usage Profile
- Time Profile - Search by a specific Time Profile.

- Guest Role - Search by a specific Guest Role.
 - Event Code - Search by a specific Event Code.
 - Inactive—Select this option to include search for Inactive accounts.
 - Active—Select this option to include search for Active accounts.
 - Expired—Select this option to include search for Expired accounts.
 - Suspended—Select this option to include search for Suspended accounts.
 - Pending Approval - Used when creating Event Codes, this will list accounts pending approval by Sponsor.
 - Rejected -Used when creating Event Codes, this will list accounts rejected by Sponsor.
3. Click the Run button to search based on the given criteria. If your search criteria matches any accounts in the database, they are displayed.
 4. Click the Save as Default option to save your current search as a default search.
 5. Click on the Reset to Default option if you have made other searches and wish to revert back to your saved default search.
 6. Click on Download as CSV if you wish to download your search as a CSV file.

Suspending Guest Accounts

You can terminate an account so that a User can no longer login. To do this, you need to contact your network administrator to make sure that the user has been removed from the network. Depending on the access method, this may happen automatically. Suspending does not delete the account, but marks the account as suspended so that it cannot be used anymore.



Note: Account suspension will only work if the controller in use supports 'Change of Authorization'.





















1. Select Account Management > Report and Manage Accounts as shown below.

Report & Manage Accounts

Created By: meru networks; Status: Inactive,Active,Pending Approval; Active Time between 02-Nov-2014 00:00 and 02-Jan-2015 00:00 [Advanced Search >>](#)

[Run](#) [Save as Default](#) [Reset to Default](#) [Download CSV](#)

Showing 1-10 of 51 10 per page Go

<input type="checkbox"/>	Created By ▲▼	Username ▲▼	MAC Address ▲▼	Password ▲▼	First Name ▲▼	Last Name ▲▼	Status ▲▼	Start Time ▲▼	End Time ▲▼	
<input type="checkbox"/>	meru networks	meru@meru.com		5aj8gehg	User	One	Active	02-Dec-2014 14:28 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	 
<input type="checkbox"/>	meru networks	BjCG6NH7		tm09wpm6			Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	 
<input type="checkbox"/>	meru networks	nc379Qet		ggk2ra3b			Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	 
<input type="checkbox"/>	meru networks	rPPYU3rd		jk0vr03t			Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	 
<input type="checkbox"/>	meru networks	Fqpk23af		9ex5kci			Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	 
<input type="checkbox"/>	meru networks	5K8vF0zh		w03fbv7k			Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	 
<input type="checkbox"/>	meru networks	y5Xa9Q7f		zq3prwo3			Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	 
<input type="checkbox"/>	meru networks	Klma89mU		9lbulu4d			Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	 
<input type="checkbox"/>	meru networks	w77g7uHp		an0wo9b			Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	 
<input type="checkbox"/>	meru networks	6UQ7kVwP		xyme6b0x8			Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	 

[Suspend All](#)

Page 1 of 5 Go

- Click the suspend icon next to the account you want to terminate. The account is removed from the list and the User will not be able to login anymore.
- To Suspend more than once account, place a check in the check box of each account you wish to suspend and then click on the Suspend All button to suspend the selected accounts.

Note: You can revive the account at a later date by performing an advanced search for suspended accounts and clicking on the revive account icon.

Charging and Refunding Transactions on Purchased Guest Accounts

If a User has purchased an account through a Guest Portal using the Payment Provider option, you can now charge or refund that Users payment if necessary.

1. Go to Account Management --> Report and Manage Guests

Report & Manage Accounts

Status: Inactive,Active,Pending Approval: Active Time between 17-Nov-2014 00:00 and 17-Jan-2015 00:00 [Advanced Search >>](#)

[Run](#) [Save as Default](#) [Reset to Default](#) [Download CSV](#)

Showing 1-5 of 5 10 per page [Go](#)

<input type="checkbox"/>	Created By ▲▼	Username ▲▼	MAC Address ▲▼	Password ▲▼	First Name ▲▼	Last Name ▲▼	Status ▲▼	Start Time ▲▼	End Time ▲▼	
<input type="checkbox"/>	local	mgM6t8Bk		shBa7eum			Active	17-Dec-2014 06:18 America/Los_Angeles	17-Dec-2014 23:59 America/Los_Angeles	
<input type="checkbox"/>	local		ae1bccc11-22-33		test	device	Active	17-Dec-2014 06:31 America/Los_Angeles	17-Dec-2014 23:59 America/Los_Angeles	
<input type="checkbox"/>	identitynetworks.com	dfuser1			DFuser1	Last Name	Active	17-Dec-2014 11:54 Europe/London	17-Dec-2014 23:54 Europe/London	
<input type="checkbox"/>	identitynetworks.com	dfuser2			DFuser2		Active	17-Dec-2014 12:07 Europe/London	18-Dec-2014 00:07 Europe/London	
<input type="checkbox"/>	login	test@test.com2		Bsp6RH8H	aanjum		Active			

[Suspend All](#)

2. Click on the Currency Unit Icon as shown on the far right, and this will display the screen below.

Charge/Refund & Payments Report: test@test.com2

Showing 1-4 of 4 10 per page [Go](#)

Transaction ID	Customer	Guest Portal	Payment Account	Access Plan	(USD) Amount ▲▼	Date ▲▼
2225724394	aanjum	login	Auth	plan1	2.00 = 2 + 0 @0%	17-Dec-2014 06:29:17
Added By: local					5.00	17-Dec-2014 06:37:01
Added By: local					5.00	17-Dec-2014 08:54:55
Added By: local					-2.00	17-Dec-2014 08:54:58

[Page 1 of 1](#) [Go](#)

Transaction Type: ☒ Charge
☐ Refund

Amount: (USD)

Reason:

Note: Manually added transactions are only recorded for the guest. they are not charged/refunded on the payment system. This must be done manually in the relevant payment systems interface.

[Add](#) [Cancel](#) [Send Purchase Receipt](#)

3. This displays the Transaction ID and the history related to it. To refund a payment :

- Transaction Type - Click on the Charge or Refund option depending on which you wish to do.
- Amount - Enter the amount you wish to charge or refund.
- Reason - Enter a reason for the charge or refund.
- Click Add to add the charge the User or refund the User.

Creating Event Codes

FortiConnect has the ability to allow a sponsor to create Event Codes which would allow Users to create their own accounts when they were invited to an Event and the code generated by the Sponsor was given to them. The Users would be subject to the timeout of that Code depending on how long an Event was created for, be it a morning seminar or a week long conference.

Event Codes can be created in the Sponsor interface and then issued to Users who will then access the Hotspot created for that Event and self register.

If you have the correct permissions to set up Event Codes, you will see the the options to Create and Manage Event codes at your Getting Started screen :-

Creating Event Codes

To create an Event Code goto Event Codes --> Create Event Codes.

Create Event Code

Details

Code Name:

Description:

Accounts can be created between:

And:

Timezone:

Account Limit:

☒ Maximum Created Accounts Maximum number of accounts that can be created for this event

☐ Maximum Active Accounts Maximum number of accounts that can be active at any one time

Note: You will only see this option if your Administrator has given you the relevant permissions

1. Enter the following information in the fields provided
 - Code Name - Enter the Name of the Code that will be provided to your Users.
 - Description - Enter a Description of the Event
 - Accounts can be created between - From the drop down menus and date pickers, select the start and end dates you wish Users to be able to create their own accounts.
 - Timezone - Enter the Timezone that event will occur in.
 - Account Limit - Maximum Created Accounts - Enter the maximum number of accounts that can be created for the Event.
 - Account Limit - Maximum Active Accounts - Enter the maximum number of accounts that can be active at anyone time for the Event.
2. Click on Create Event Code when complete.
3. Once this has been completed you will see an extra tab appear, Time Restrictions, you can use this screen to restrict Users from creating their accounts between certain times.
4. Click on the Time Restrictions tab as shown below.

Edit Event Code

Details **Time Restrictions**

Guests cannot create their accounts using this event code during these periods

No current restrictions for this event code

Monday 00 00 23 59 **Add**

5. Enter the restrictions you wish to impose using the drop down tabs provided and click on Add after each one.

You are now ready to issue your Event Code to Users so that they can Self Register when ready

Managing Event Codes

Click on Manage Event Codes in the Event Codes section.




1. From the Manage Events Code page you can tailor and run a report using the fields provided as shown below.

Managing Event Codes

Manage Event Codes

Created By: Active Time Between: 2 Nov 2014

Code Name: And: 1 Jan 2015

Created By ▲▼	Code Name ▲▼	Status ▲▼	Accounts can be created between ▲▼	And ▲▼	Account Group ▲▼	Usage Profile ▲▼	
meru networks	Event_One	Active	02-Dec-2014 14:54 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	Default Account Group	default	  

Showing 1-1 of 1 10 per page Go




Page 1 of 1 Go

- This will list all the event codes that have been created and then can be managed accordingly -
 - Click on the suspend icon to suspend the Event.

Manage Event Codes

Created By: Active Time Between: 2 Nov 2014

Code Name: And: 1 Jan 2015

Created By ▲▼	Code Name ▲▼	Status ▲▼	Accounts can be created between ▲▼	And ▲▼	Account Group ▲▼	Usage Profile ▲▼	
meru networks	Event_One	Active	02-Dec-2014 14:54 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	Default Account Group	default	  

Showing 1-1 of 1 10 per page Go

Page 1 of 1 Go

The page at 192.168.137.20 says:

Are you sure you want to suspend this event code?

- Click on the edit icon to edit the details of the Event.

Edit Event Code

Details

Time Restrictions

Code Name:

Event One

Description:

test

Accounts can be created between:

2

Dec

2014

14

54

And:

2

Dec

2014

23

59

Timezone:

America/Los_Angeles

Account Limit:

☒ Maximum Created Accounts

20

Maximum number of accounts that can be created for this event

☐ Maximum Active Accounts

Maximum number of accounts that can be active at any one time

Edit Event Code

Cancel

Edit any changes and click on Edit Event Code to confirm.

- Click on the view accounts icon to view the Users that have created their own accounts for the Event so far.

Report & Manage Accounts

Event Code: Event One; Active Time between 02-Dec-2014 14:54 and 02-Dec-2014 23:59

Sponsor Group:
Created By:
Guest Portal:
Username:
MAC Address:
First Name:
Last Name:
Company:
Email:
Mobile Phone Number:
Inactive: ☐
Active: ☐
Expired: ☐
Suspended: ☐
Pending Approval: ☐
Rejected: ☐

Active Time Between:
And:
Timezone:
IP Address:
Usage Profile:
Account Group:
Event Code:

<input type="checkbox"/>	Created By	Username	MAC Address	Password	First Name	Last Name	Status	Start Time	End Time
No Records Found									

To perform an advanced search click on the Advanced Search Button as shown below under Account Management-->Report & Manage Accounts.

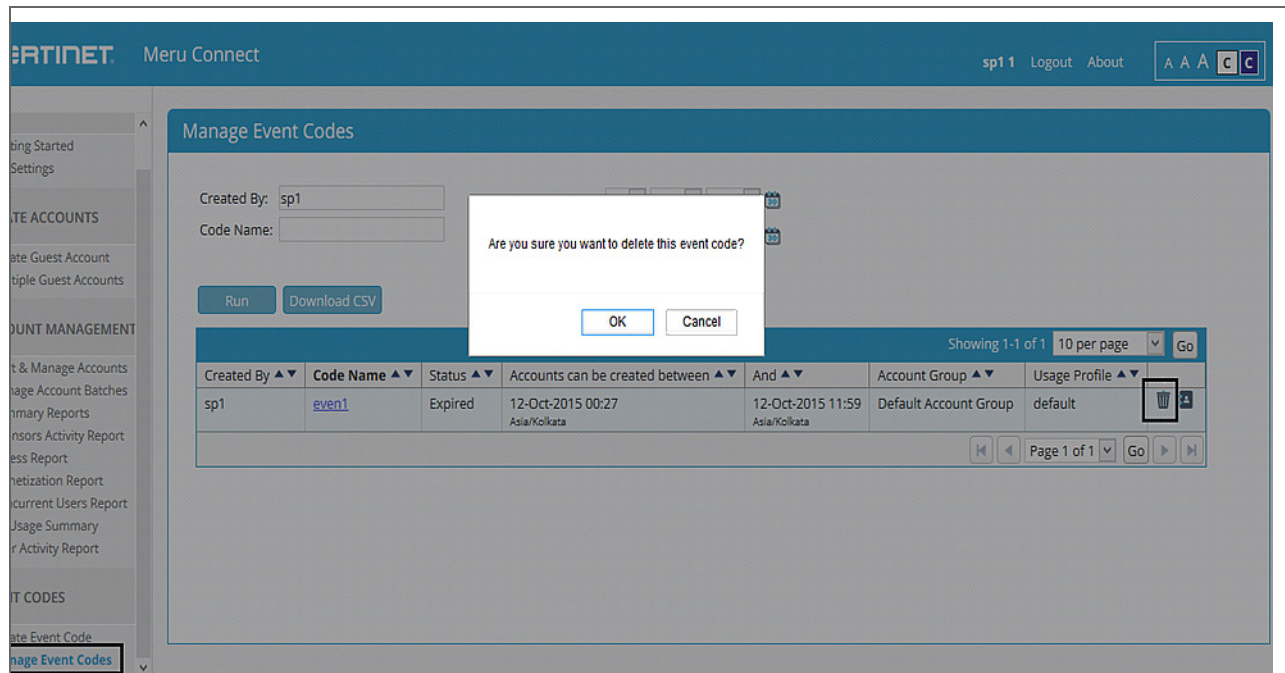
Searches can be made using the relevant search criteria entered into the correct search fields.

Delete expired event codes

A sponsor can delete an expired event code from the **Manage event codes** page. Sponsor should have "Manage Event Codes" permission to delete expired event code.

Step 1 Select Event Codes > Manage Event Codes.

Step 2 Click Delete icon next to the event code to delete the event code



Viewing Active Accounts and Resending Details

FortiConnect provides an Active Accounts page that allows you to view the active accounts that you created or accounts that you have permissions to view. This page allows you to view, print, email or text message (SMS) the account access details to Users if they have lost or forgotten them.

1. Select Account Management > Report & Manage Guests to display a list of active accounts.
2. Click the username of the User to which you wish to resend details as shown below.

Guest Account Details

Username:	test@test.com2
Password:	Bsp6RH8H
Status:	Active
Maximum Duration:	1 hour(s), 0 minute(s)
First Name:	aanjum
Last Name:	Not available
Company:	Not available
Email Address:	test@test.com
Mobile Phone Number:	+44 00000000000
Usage Profile:	1 Hour
Account Group:	Default Account Group

[Print Account](#)[Email Account](#)[Send SMS Message](#)[Suspend](#)[Send Purchase Receipt](#)[Reset Password](#)

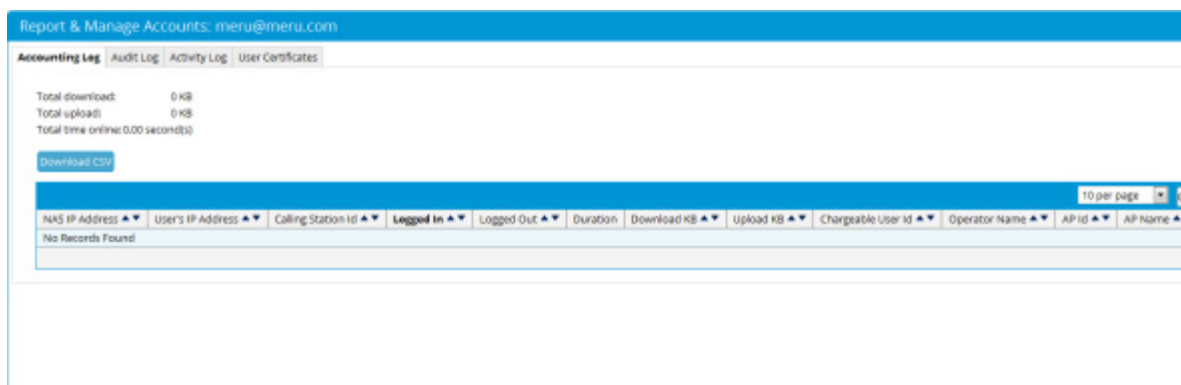
From this page you can click the relevant buttons:

- **Print Account**—Prints the account.
- **Email Account**—Sends email the account to the User.
- **Send SMS Message**—Sends an SMS message of the account details to the User.
- **Suspend** —Suspend the User account.
- **Send Purchase Receipt** - Resend a Purchase receipt to a purchased account.

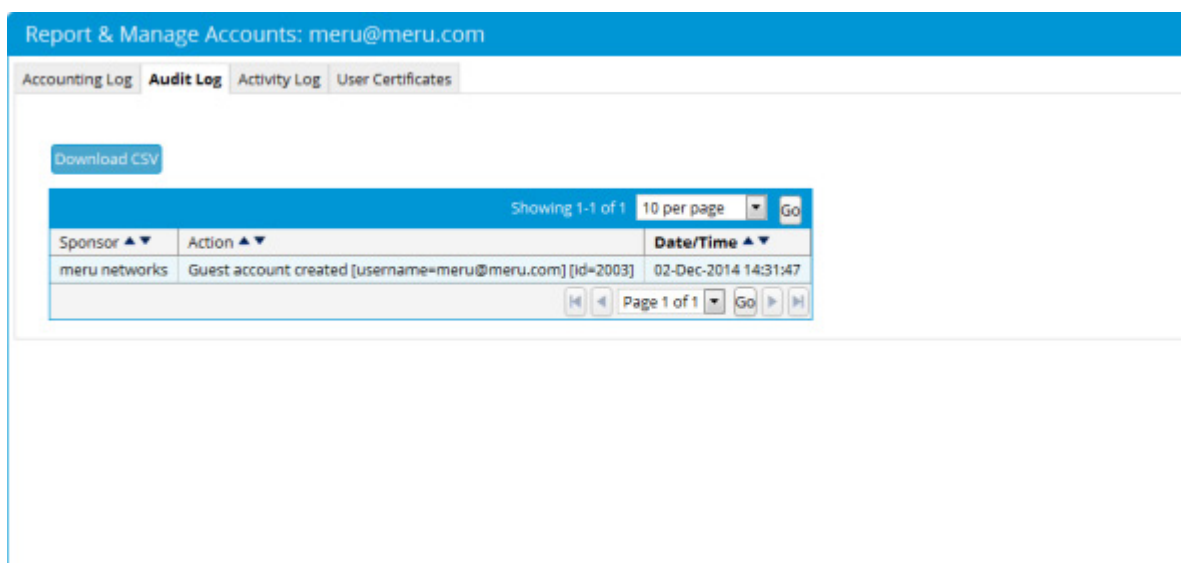
Reporting on Guest Users

If you have the appropriate permissions, you can generate full reporting on User user accounts. You can run reports to view who created User accounts, when they were created, and access details for the Users themselves, such login time, logout time, and IP address used.

1. From the Main page, select Account Management > Report & Manage Guests to display a list of active accounts as shown below.
2. Select the user for which you wish to view reporting, and click the notepad icon to view the detailed report for that user.
3. Click the Accounting Log tab as shown below for the RADIUS accounting information for that User including:
 - Total Download - Total Download Usage in KB
 - Total Upload - Total Upload Usage in KB
 - Total Time Online
 - NAS IP Address—NAS IP address the User user was specified.
 - Users IP Address—IP Address assigned to the User.
 - Logged In—Time at which the User logged in.
 - Logged Out—Time at which the User logged out.
 - Duration—Duration of time the User remained logged in the account.
 - Download KB - Total amount of data downloaded by User.
 - Upload KB - Total amount of data uploaded by User.
 - Chargeable User ID - The Chargeable User ID attached to the account
 - Operator Name - Operator Name of the account
 - AP ID - AP ID account came via
 - AP Name - AP Name account came via



4. Click the Audit Log tab as shown below to view the audit entries for that User account including:
 - Sponsor—Sponsor ID.
 - Action—Audit entry action.
 - Date/Time—Date and Time of audit entry action.



5. Click the Activity Log tab as shown below to view the activities performed by the User for that account, including firewall information if your administrator has allowed that functionality.

Report & Manage Accounts: Fqpk23ef

Accounting Log Audit Log **Activity Log** User Certificates

Activity Data last loaded 02-Dec-2014 16:02:44 Refresh

Network Device IP:

Message Contains:

Use regular expression: ☐

Between: 2 Nov 2014 16:02 And: 2 Dec 2014 16:02

Run Download CSV

10 per page Go

Date/Time ▲▼	Device ▲▼	Message ▲▼
No Records Found		

Search criteria include:

- Network Device IP—IP address of any network device you wish to search.
- Message Contains—Enter any text you wish to search for within the logs.
- Use regular expression—Check this checkbox to search for the specified text that matches with regular expression. You can use Perl compatible regular expressions in the search.
- Between—Enter Date and Time from which you want to start your search.
- And—Enter Date and Time at which you want to end your search.

6. Click the Run button once you have completed selecting your criteria. Once the search is completed, you can click the Download button to save your results to a file.

Returned information includes:

- Date/Time field—Displays the date and time of the User's actions.
- Device—The device on which the User's actions took place.
- Message—Displays the User's actions.

Creating Device Accounts

If you are assigned the appropriate permissions, you can create temporary device accounts.

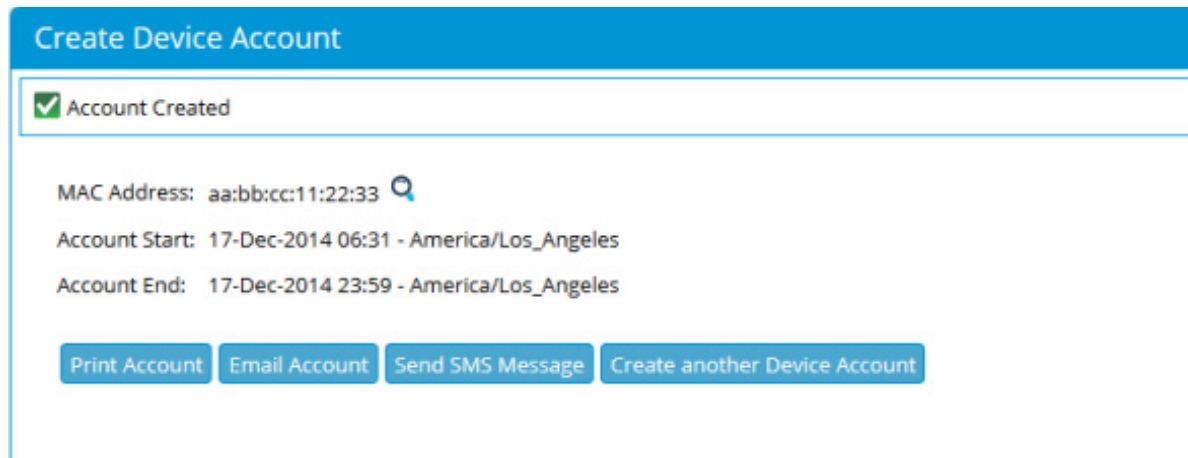
1. Log into the FortiConnect as described in [Connecting to the FortiConnect](#).
2. Navigate to **Create Accounts > Create Device Account**.
3. The Create Device Account page appears as shown in [Figure devaccpage](#).

Note: The screenshot below shows the default template for creating a Device Account. Your administrator has the option to add or remove other fields.

The screenshot shows the 'Create Device Account' form. It has a blue header bar with the title 'Create Device Account'. Below the header, there are several input fields and dropdown menus. The fields are: MAC Address, First Name, Last Name, Company, Email Address, Mobile Phone Number (with a dropdown for country code, currently showing '+1'), Timezone (dropdown, currently showing 'America/Los_Angeles'), Account Start (with date and time dropdowns, currently showing '2 Dec 2014' and '16 04'), and Account End (with date and time dropdowns, currently showing '2 Dec 2014' and '23 59'). At the bottom of the form are two buttons: 'Add Device' and 'Cancel'.

4. Enter the MAC Address of the device then follow the steps below to enter the details of the User requesting the device be added onto the network.
5. Enter the First Name of your User.
6. Enter the Last Name of your User.
7. Enter the Company or organization of your User. Enter the Email Address of your User.
8. Enter the Mobile Phone Number of your User.
9. Select the Guest Role from the dropdown menu. This dropdown appears automatically if your administrator has defined User roles and more than one role is available.

10. Choose the Timezone relevant to the time and date.
11. From the Account Start field, choose the Time and Date from which you want the account to be valid.
12. From the Account End field, choose the Time and Date at which you want the account to end.
13. If the administrator for FortiConnect has configured any additional required account attributes, specify the appropriate information for those settings in this form.
14. Click the Add Device button. The account is created and the details are displayed as shown below.



The screenshot shows a web interface titled "Create Device Account". Below the title bar, there is a green checkmark icon followed by the text "Account Created". Below this, the following details are displayed:

- MAC Address: aa:bb:cc:11:22:33 (with a magnifying glass icon)
- Account Start: 17-Dec-2014 06:31 - America/Los_Angeles
- Account End: 17-Dec-2014 23:59 - America/Los_Angeles

At the bottom, there are four blue buttons: "Print Account", "Email Account", "Send SMS Message", and "Create another Device Account".

15. Depending on your permissions, you can perform one or all of the following actions on the same page where the new account details are displayed:
 - Clicking the Print Account button allows you to print the account details to your printer to hand to the User. These details commonly include User access instructions and usage policies. See Print Account Details.
16. You can also create another account immediately by clicking the Create another Device account button.

Multiple Device Accounts

The FortiConnect allows you to create multiple device accounts at the same time. The options available to you are configured by your administrator. They include:

- Creating Multiple Device Accounts from Text Entry
- Creating Multiple Device Accounts from CSV File

You can create multiple accounts by pasting the details into the interface or importing a Comma Separated Values (CSV) file.

Creating Multiple Device Accounts from Text Entry

1. Navigate to Create Accounts--> Multiple Device Accounts as shown below

[illegible]

2. Enter the details in the grid fields as required with a cell separating the values.
3. Select the **Guest Role** from the dropdown menu. This dropdown appears automatically if your administrator has defined User roles and more than one role is available.
4. Select the relevant Timezone for the account.
5. Choose the **Account Start time**, and then the **Account End time**.
6. Click the **Create Accounts** button.

Creating Multiple Device Accounts from CSV File

1. Navigate to Create Accounts > Multiple Device Accounts as shown below.

	MAC Address	First Name	Last Name

2. Download the CSV file by clicking the Download Template link and save this file locally.
3. Fill out the fields in the CSV Template file using a program such as Microsoft Excel:
 - **MAC Address** - The device MAC Address.
 - **First Name** – The User's first name requesting the device be added.
 - **Last Name** – The User's last name requesting the device be added.
 - **Company** – The User's company requesting the device be added.
 - **Email Address** – The User's email address requesting the device be added.
 - **Country Code** - The country code of the mobile phone number, for example 1 for the US, 44 for the UK.
 - **Mobile Phone Number** – The User's mobile phone number requesting the device be added.
NOTE: Do not enter hyphens in the number.
 - **Other details** - Other details may be configured by your administrator and the names and descriptions are decided by them.
4. Save the CSV Template file in CSV format.
5. Click the **Browse** button to select your edited CSV file.

6. Select the **Guest Role** from the dropdown menu. This dropdown appears automatically if your administrator has defined Usage Profiles and more than one profile is available.
7. Select the relevant Timezone for the account.
8. Choose the Account Start time, and then the Account End time.
9. Click the **Import** button.

Managing Device Accounts































You can view all accounts that have been created at any time.

1. From the Main page select Account Management > Report and Manage Accounts.
2. On the Manage Devices page, you can view the list of accounts that have been created as shown below. The fields displayed on this page can be customized using Report Settings.

Report & Manage Accounts

Created By: meru Status: Inactive,Active,Pending Approval Active Time between 02-Nov-2014 00:00 and 02-Jan-2015 00:00 [Advanced Search >>](#)

[Run](#) [Save as Default](#) [Reset to Default](#) [Download CSV](#)

	Created By	Username	MAC Address	Password	First Name	Last Name	Status	Start Time	End Time	
<input type="checkbox"/>	meru		1e2d81ad21121	test	test		Active	02-Dec-2014 16:04 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	  
<input type="checkbox"/>	meru networks	meru@meru.com		Saj8geh9	User	One	Active	02-Dec-2014 14:28 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	  
<input type="checkbox"/>	meru networks	BjCG0NH7		tm9wpm6			Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	  
<input type="checkbox"/>	meru networks	nx3Z8Qec		ggk2ra3b			Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	  
<input type="checkbox"/>	meru networks	rFPYU3n4		jk0vrl3t			Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	  
<input type="checkbox"/>	meru networks	Fopk23ef		9exd5ci			Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	  
<input type="checkbox"/>	meru networks	5k8vf12b		wo3fbv7k			Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	  
<input type="checkbox"/>	meru networks	y5xw9Q1f		zq3prwo3			Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	  
<input type="checkbox"/>	meru networks	Klm49mJ		9lbulu4d			Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	  
<input type="checkbox"/>	meru networks	w77g7uHp		ani8wo9b			Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	  

Showing 1-10 of 52 10 per page [Go](#)

Page 1 of 6 [Go](#)

Editing Device Accounts

If you create an account for a device and you need to extend its account access, you can change the expiry date and time of the account.































1. From the Main page select Account Management > Report and Manage Accounts.

Report & Manage Accounts

Created By: meru Status: Inactive,Active,Pending Approval Active Time between 02-Nov-2014 00:00 and 02-Jan-2015 00:00 [Advanced Search >>](#)

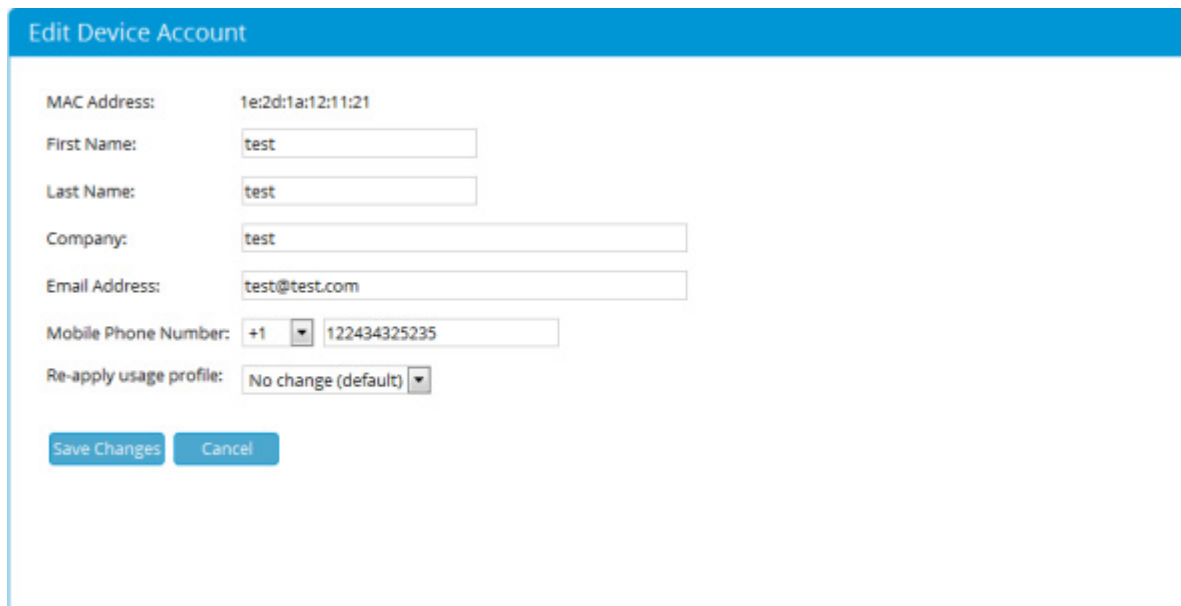
[Run](#) [Save as Default](#) [Reset to Default](#) [Download CSV](#)

Showing 1-10 of 52 10 per page [Go](#)

<input type="checkbox"/>	Created By ▲▼	Username ▲▼	MAC Address ▲▼	Password ▲▼	First Name ▲▼	Last Name ▲▼	Status ▲▼	Start Time ▲▼	End Time ▲▼	
<input type="checkbox"/>	meru		1e2d1a12:1121		test	test	Active	02-Dec-2014 16:04 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	  
<input type="checkbox"/>	meru networks	meru@meru.com		Saj@gehg	User	One	Active	02-Dec-2014 14:28 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	  
<input type="checkbox"/>	meru networks	BjCG9NH7		tm9wpm6			Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	  
<input type="checkbox"/>	meru networks	nx329Qet		gpk2ra3b			Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	  
<input type="checkbox"/>	meru networks	rPPVJ3r4		jk0vrl3t			Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	  
<input type="checkbox"/>	meru networks	Fgpk23ef		9exl5ci			Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	  
<input type="checkbox"/>	meru networks	5K0vf12b		wo3fbv7k			Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	  
<input type="checkbox"/>	meru networks	y5xa9Q1f		zq3prwo3			Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	  
<input type="checkbox"/>	meru networks	Klm49mj		9lbuk4d			Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	  
<input type="checkbox"/>	meru networks	w7Tg7uHp		anl8wo9b			Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	  

Page 1 of 6 [Go](#)

2. Click the pencil icon next to the account you want to change to go to the Edit Device Account page as shown below.



MAC Address: 1e:2d:1a:12:11:21

First Name: test

Last Name: test

Company: test

Email Address: test@test.com

Mobile Phone Number: +1 122434325235

Re-apply usage profile: No change (default)

Save Changes Cancel

3. Change the Account details.
4. Click the Save Changes button to update the account with the new details.

Advanced Device Search

1. If your Account Management page returns a large number of devices, you can perform an advanced search by clicking the **Advanced Search button** as shown below.

Report & Manage Accounts

Created By: meru; Status: Inactive,Active,Pending Approval; Active Time between 02-Nov-2014 00:00 and 02-Jan-2015 00:00 << Advanced Search

Sponsor Group:	All	Active Time Between:	2 Nov 2014
Created By:	meru		00 00
Guest Portal:		And:	2 Jan 2015
Username:			00 00
MAC Address:		Timezone:	All
First Name:		IP Address:	
Last Name:		Usage Profile:	
Company:		Account Group:	
Email:		Event Code:	
Mobile Phone Number:			

☒ Inactive
☒ Active
☐ Expired
☐ Suspended
☒ Pending Approval
☐ Rejected


2. In the Advanced Search page that is displayed, you can enter the **following** criteria to make your search:
 - Created by—Sponsor who created the account.
 - MAC Address - MAC Address of device
 - First Name—First Name of User.
 - Last Name—Last name of User.
 - Company—Company or Organization of User device.
 - Email—Email address of User device.
 - Start Time Between—Start Time from which the search to start.
 - End Time Between—End Time at which the search to end.
 - Timezone—From the dropdown menu select a timezone to be searched.
 - Inactive—Select this option to include search for Inactive accounts.
 - Active—Select this option to include search for Active accounts.
 - Expired—Select this option to include search for Expired accounts.
 - Suspended—Select this option to include search for Suspended accounts.
3. Click the **Run** button to search based on the given criteria. If your search criteria matches any accounts in the database, they are displayed.
4. Click the **Save as Default** option to save your current search as a default search.

- Click on the Reset to Default option if you have made other searches and wish to revert back to your saved default search.
- Click on Download as CSV if you wish to download your search as a CSV file.

Note: Remember that not all device search criteria will be relevant to that of a User search.

Suspending Device Accounts

You can terminate an account so that a device can no longer login. Depending on the access method, this may happen automatically. Suspending does not delete the account, but marks the account as suspended so that it cannot be used anymore.

 **Note:** Account disconnection will only work if the controller in use supports 'Change of Authorization', suspension of accounts will always work.































- Select Account Management > Manage Devices as shown below.

Report & Manage Accounts

☒ Selected guest account(s) suspended

Created By: meru; Status: Inactive,Active,Pending Approval; Active Time between 02-Nov-2014 00:00 and 02-Jan-2015 00:00
 [Advanced Search >>](#)

[Run](#)
[Save as Default](#)
[Reset to Default](#)
[Download CSV](#)

	Created By	Username	MAC Address	Password	First Name	Last Name	Status	Start Time	End Time	
<input type="checkbox"/>	meru networks	BjCG2Nt7		tm9wpm6			Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	  
<input type="checkbox"/>	meru networks	nx3Z9Qst		ggk2ra3b			Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	  
<input type="checkbox"/>	meru networks	rPPYU3t4		jk6vr13t			Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	  
<input type="checkbox"/>	meru networks	FqpkT3ef		9exl5ci			Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	  
<input type="checkbox"/>	meru networks	5K8vF2h		wo3fbv7k			Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	  
<input type="checkbox"/>	meru networks	y5Xe9QIf		zq3prwo3			Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	  
<input type="checkbox"/>	meru networks	KIm4f9mJ		9lbulu4d			Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	  
<input type="checkbox"/>	meru networks	w7Tg7uHp		an8wo9b			Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	  
<input type="checkbox"/>	meru networks	6UQ7jKwQ		xyme6bx8			Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	  
<input type="checkbox"/>	meru networks	b4chm3eJ		gade9gq4			Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	  

[Suspend All](#)

2. Check the check box of the accounts you wish to suspend then Click the Suspend All button. The account is removed from the list and the device will not be able to login anymore.

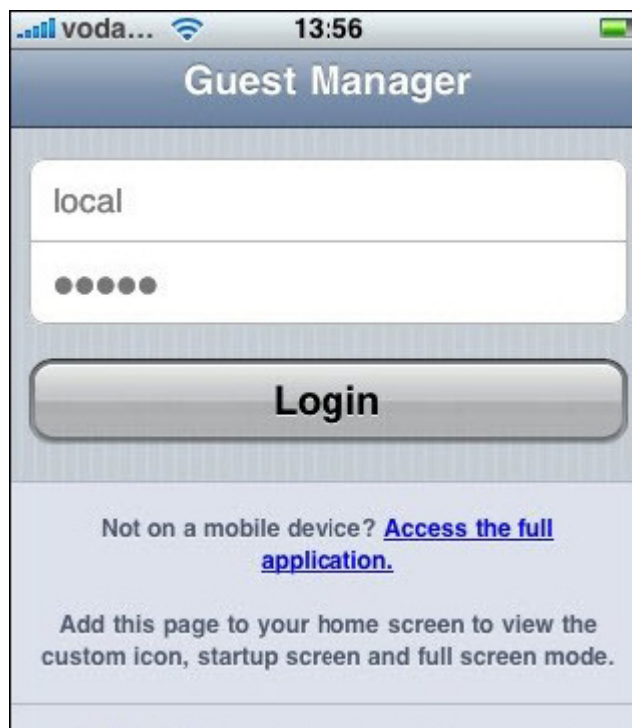
Mobile Device User Interface

Sponsors can create Users using a mobile device as long as the sponsor has the correct administrative permissions to create accounts.

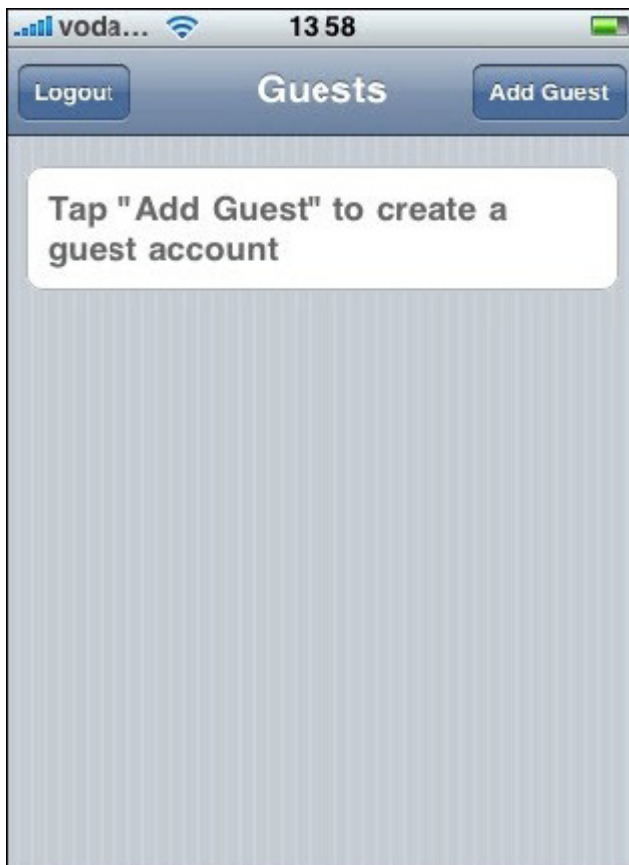
Note: Compatible with I-Phones, Android and Blackberrys. Although some older browsers on these devices may not support the Mobile User Interface.

Note: Screenshots below are of the I-Phone and may differ on other Mobile Devices

1. Using your Mobile device, navigate to your FortiConnect Management browser as shown below.



2. Enter your Username and Password in the fields provided and tap on the Login button, this should bring up the Mobile UI home page as shown below.



3. Tap on the Add Guest button to create a User account and enter the information required in the fields provided as shown below.



The screenshot displays a mobile application interface for adding a guest. At the top, the status bar shows 'voda...', signal strength, Wi-Fi, and the time '13:58'. The app's header features a 'Back' button and the title 'Add Guest'. The main content area contains a series of input fields: 'First Name', 'Last Name', 'Company', 'Email Address', '+1 Mobile Phone Number', a dropdown menu with 'default' selected and a right arrow, and a time field set to 'Ends today at 07:00' with a right arrow. A large, rounded 'Add' button is positioned at the bottom of the form.

4. In the fields provided enter the following :-

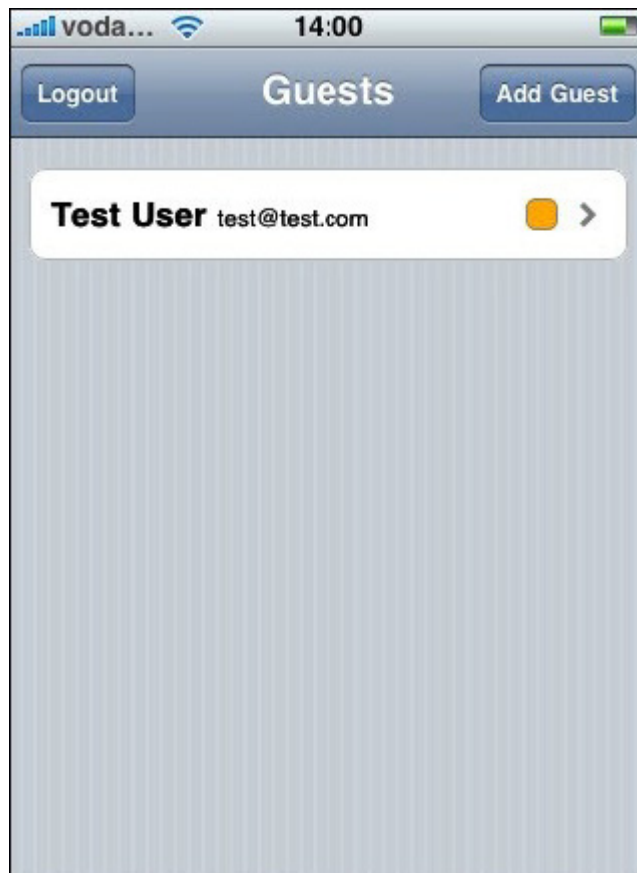
- First Name - First Name of the User user
- Last Name - Last Name of the User user
- Company - Company name of the User user
- Email Address - Email Address of the User user
- Mobile Phone Number - Users mobile phone number
- Group - Default by standard, but tap the > icon to see more groups if applicable.
- End time - Tap the > icon to select a time you wish the users access to end by.

Tap on the Add button once complete.

5. Once you have selected Add the user details will show as per below.



6. Tap on the Back button to return back to your Mobile UI home screen.



7. To check the status of any of the Users you have created on your Mobile UI home screen tap on the > icon next to the User.



Once you have finished with your Mobile UI, tap the Logout button on the Mobile UI home page to logout.

Concurrent Users Report

A Sponsor may also be able to run a report on Users that are concurrently connected to the Network at any one time and see license usage and licenses used over a specific period.

1. From the Sponsor User Interface, go to Account Management-->Concurrent Users Report as shown below.

Concurrent Users Report

View Between: 25 Nov 2014

And: 2 Dec 2014

Username:

MAC Address:

Created By: meru

Enter either the sponsor's username or the user's domain name

Show Connected Only: ☐

Run

10 per page Go

Created By ▲▼	Username ▲▼	MAC Address ▲▼	Logged In ▲▼	Logged Out ▲▼	IP Address ▲▼	NAS IP Address ▲▼
No Records Found						

2. Select which dates you wish to run the report from and to using the View Between date picker.
 - License Type - To run a report on a specific license type use the drop down menu to select.
 - Username - To run a report on a specific User enter the username of the User. Leave blank to search for all.
 - MAC Address - To run a report on a MAC address enter the MAC address details here.
 - Created by - To run a report on Users created by a specific sponsor enter the sponsors username, leave blank to search for all.
 - Show Connected Only - Place a check in the check box to show connected Users only
3. Once the report has run, a list of connected Users will appear.
 - Click the Link icon to disconnect the active User from the Network.
 - Click the suspend icon to suspend the Users account.

Concurrent Guests Report

View Between: 10 Dec 2014
And: 17 Dec 2014
Username:
MAC Address:
Created By:
Enter either the sponsor's username or the user's domain name
Show Connected Only:
Run

Created By	Username	MAC Address	Logged In	Logged Out	IP Address	NAS IP Address	
identitynetworks.com	dfuser1	a0f4505f7eaf	17-Dec-2014 05:48		10.1.210.109	10.1.210.45	
identitynetworks.com	DFUser1 Last Name	00:1cbf0497:6b	17-Dec-2014 04:41	17-Dec-2014 04:57	10.1.210.104	10.1.210.45	
identitynetworks.com	dfuser1	00:1cbf0497:6b	17-Dec-2014 04:40	17-Dec-2014 04:41	10.1.210.104	10.1.210.45	
identitynetworks.com	dfuser2	30:85:a9:62:64:cf	17-Dec-2014 04:38		10.1.210.105	10.1.210.45	
identitynetworks.com	DFUser2	c8:85:50:89:34:b8	17-Dec-2014 04:37		10.1.210.103	10.1.210.45	
identitynetworks.com	DFUser2	c8:85:50:89:34:b8	17-Dec-2014 04:31	17-Dec-2014 04:35		10.1.210.45	
identitynetworks.com	DFUser2	c8:85:50:89:34:b8	17-Dec-2014 04:28	17-Dec-2014 04:31		10.1.210.45	
identitynetworks.com	dfuser1	00:25:d3:bff3:2a	17-Dec-2014 04:28	17-Dec-2014 04:34	10.1.210.106	10.1.210.45	
identitynetworks.com	dfuser1	38:aa:3c:45:75:c8	17-Dec-2014 04:23	17-Dec-2014 04:35	10.1.210.108	10.1.210.45	
identitynetworks.com	DFUser2	c8:85:50:89:34:b8	17-Dec-2014 04:19	17-Dec-2014 04:28	10.1.210.103	10.1.210.45	

Showing 1-10 of 34 10 per page Go

Page 1 of 4 Go

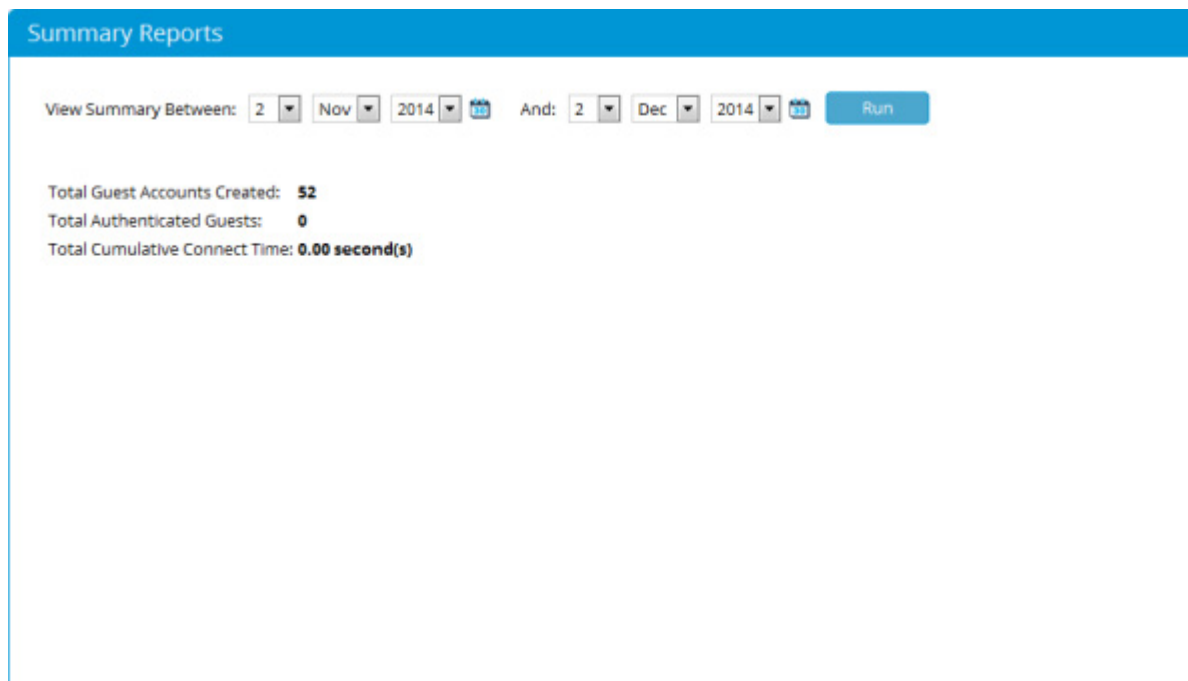
- The report will also detail the License Type and Overall License Usage below.

Sponsor Reporting

Sponsors can view reports under the Account Management section to view the summary, activity and access details for their own account and other sponsor accounts.

Summary Reports

- From the main page select Account Management > Summary Reports to bring up the summary reports page as shown below.



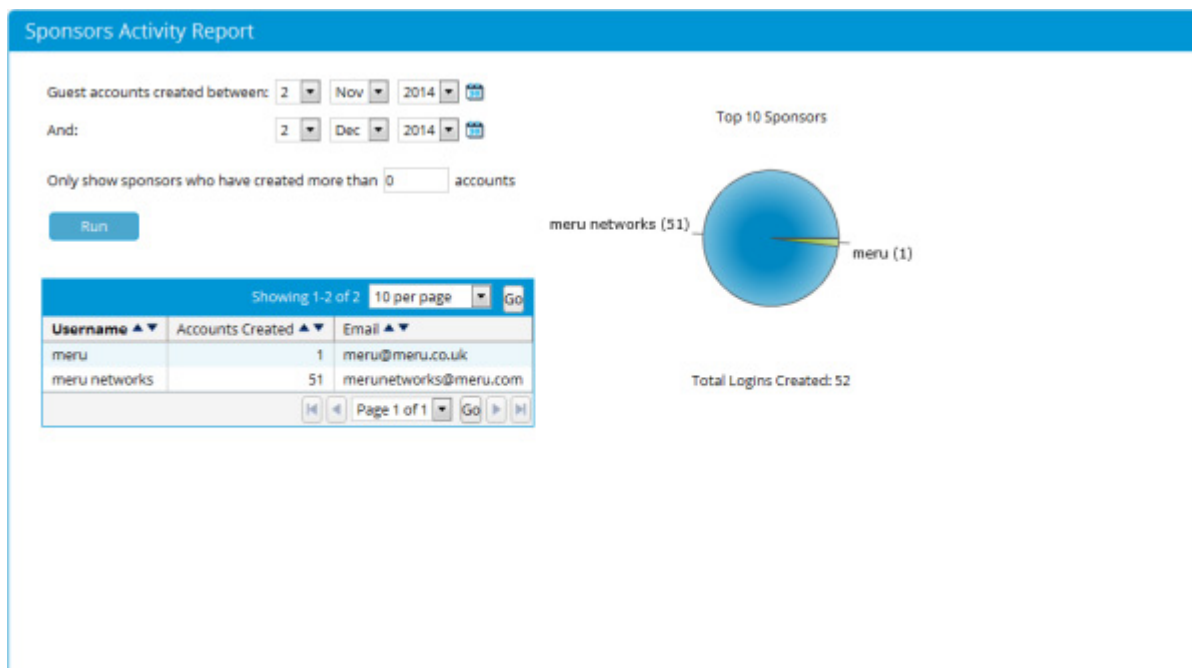
The screenshot shows a web interface titled "Summary Reports". Below the title is a search filter section with the text "View Summary Between:". This is followed by two date pickers. The first date picker is set to "2", "Nov", and "2014". The second date picker is set to "2", "Dec", and "2014". To the right of these is a blue button labeled "Run". Below the date pickers, the summary statistics are displayed:

- Total Guest Accounts Created: **52**
- Total Authenticated Guests: **0**
- Total Cumulative Connect Time: **0.00 second(s)**

2. Select a search criteria using the date pickers provided and click the Submit button.
3. The screen displays:
 - Total Guest Accounts Created.
 - Total Authenticated Guests.
 - Total Cumulative Connect Time.

Sponsors Activity Report

1. From the main page, select Account Management > Sponsors Activity Report to display the Sponsors Activity Report page as shown below.

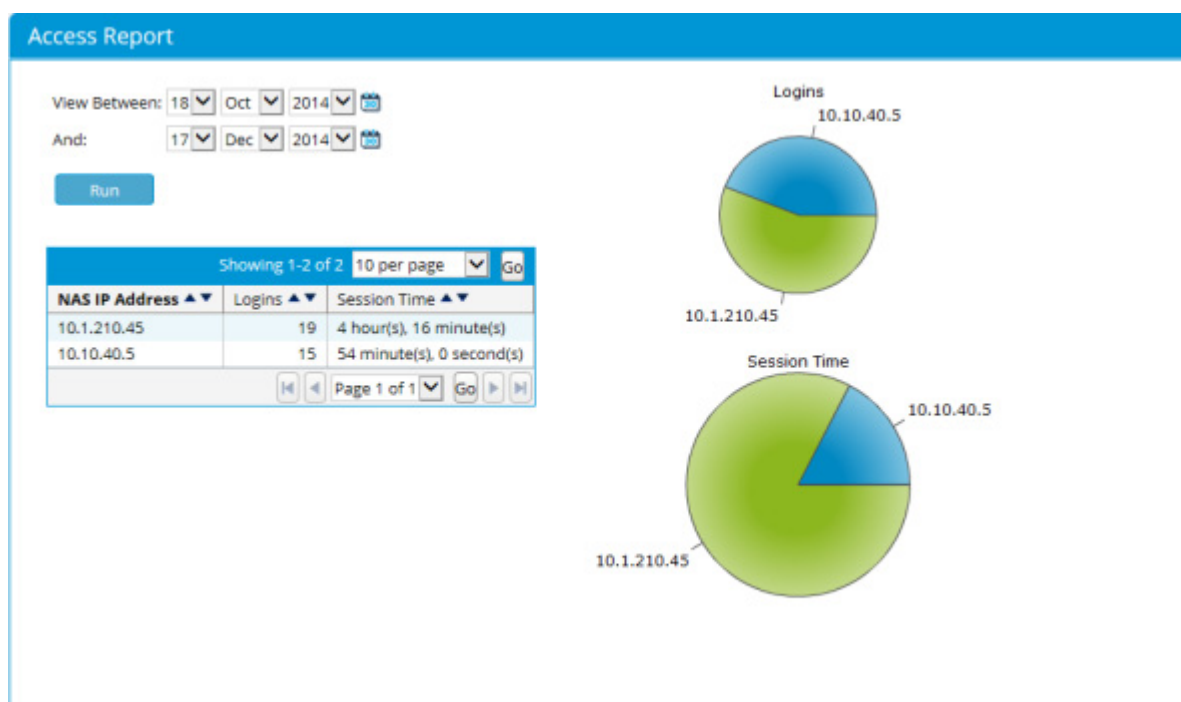


2. Select a search criteria using the date pickers provided. You can also select a minimum number of Users created by sponsor.
3. When completed, click the Run button. The screen displays:
 - Username—Username of sponsor.
 - Total Accounts Created—Accounts created by sponsor.
 - Email—Email address of sponsor.

A pie chart of the top ten sponsors, who created the accounts, is also displayed.

Access Reports

1. Navigate to Account Management > Access Report to go to the Access Report page as shown below.



2. Select a search criteria using the date pickers provided and click the Run button.
3. The screen displays the number of logins made by the enforcement device (IP Address) and its session time.

Monetization Report

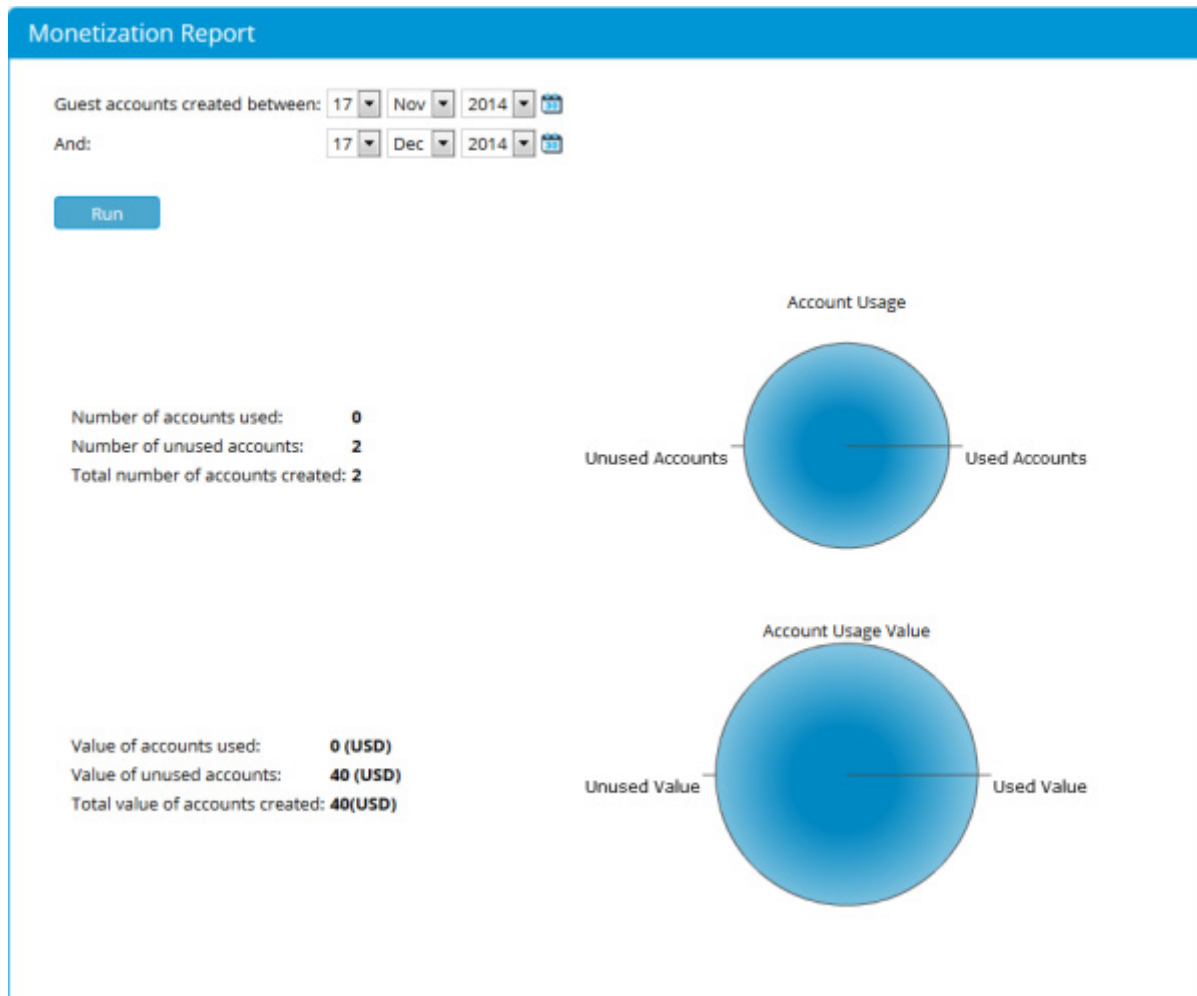
In some environments, credit card based purchases are not widely used and they are much more interested in using access codes with currency denominations attached to them.

Currency Denominations can be set up within the Admin interface, when this is set, it will allow a sponsor to create a number of random User accounts assigned to a time profile, and then export them to a CSV file to print off and then create an offline coupon or scratch card to distribute to the User.

Once the batches have been created and distributed, we can report on them using the report below.

From the Sponsor Portal go to Account Management --> Monetization Report as shown below

Monetization Report



API Support

This appendix discusses API support for the FortiConnect. It describes the following:

- Overview
- Authentication Requirements
- Time Format
- API Operations
- Status Codes
- Error Codes
- Valid Timezones

Overview

FortiConnect provides an API that allows you to perform certain operations using HTTP or HTTPS via POST or GET operations. The FortiConnect API is accessed via <https://serveripaddress/sponsor/api/GuestAccount.php> or <http://serveripaddress/sponsor/api/GuestAccount.php>.

To use this API, note the following:

- Competency with a programming language (e.g. C, Java, Perl, PHP) is required and you must install the relevant software on the machine that runs these programs to call this API.
- Fortinet does not support debugging of custom programs using the API. It only supports running API calls.

Authentication Requirements

Access over HTTP or HTTPS for the API is based upon the SSL settings for the web

Administration interface as defined in *Accessing the FortiConnect Using HTTP or HTTPS*.

A valid username and password is also required to authenticate as a sponsor against the following components:

- Local database
- Active directory server as defined in admin settings
- LDAP server as defined in admin settings
- RADIUS as defined in admin settings

For example, the following call uses the username “sponsor” with password “mypass”:

<http://1.1.1.1/sponsor/api/GuestAccount.php?username=sponsor&password=mypass&method=createCarter&email=test@merunetworks.com&role=DEFAULT&company=Meru&mobileNumber=12345484345&startTime=20100210T10%3A45%3A00&endTime=20100211T13%3A15%3A00&timezone=Europe%2FLondon&timeProfile=default>

Note: All fields must be URL encoded, e.g. date/time fields have been encoded so the colon has been replaced with %3A

Time Formats

All dates/times must be specified in a particular ISO 8601 format: YYYYMMDDTHH:MM:SS where:

- YYYY is the 4-digit year
- MM is the 2-digit month
- DD is the 2-digit day of the month
- T is a literal T
- HH is the 2-digit hour (24 hour format)
- MM is the 2-digit minute
- SS is the 2-digit second

e.g. 20100304T08:45:30 is 4 March 2010, 08:45:30

See http://en.wikipedia.org/wiki/ISO_8601 for details.

API Operations

You can use the API by passing the details either through a POST or GET operation to the Identity Manager API.

The following example shows a GET operation to obtain the version of the API and Identity Manager.

`https://1.1.1.1/sponsor/api/GuestAccount.php?`

`username=sponsor&password=mypass&method=getVersion`

All data is returned as XML.

XML Response

All responses are provided in the following XML format:

```
<?xml version="1.0"?>
<response>
  <status>
    <code>0</code>
    <message>Success</message>
  </status>
  ....
</response>
```

In the case of an error, the code and message elements are set with the error code and error text. Internal errors also return a <details> element that contains developer information to help address the issue.

create

The create method creates a guest user account in accordance with the sponsor's permissions.

Required In Parameters

- method (required): create
- username (required): Sponsor account username
- password (required): Sponsor account password
- firstName (based on policy): Guest user first name
- surname (based on policy): Guest user surname
- email (based on policy): Guest user email address
- accountGroup - name of account group (string)
- company (based on policy): Guest user company name

create Example Use

- phonecode (based on policy): Telephone code for the Guest user mobile telephone (e.g. +44)
- mobilenumber (based on policy): Mobile telephone number for the Guest user
- timezone (required): The timezone in which the guest account is created (as detailed in Valid Timezones, page A-13)
- option1 (based on policy): Optional data field 1
- option2 (based on policy): Optional data field 2
- option3 (based on policy): Optional data field 3
- option4 (based on policy): Optional data field 4
- option5 (based on policy): Optional data field 5
- startTime (required): The time the account is due to start
- endTime (required): The time the account should end
- timeProfile (required): The time profile to use when creating the account

create Example Use

1. The following example creates an account with the following guest details:

- First Name: John
- Surname: Carter
- Email: johncart@merunetworks.com
- Role: DEFAULT (as created in the user role interface)
- Company: Fortinet
- Mobile Number (cellphone): 12345 48434532
- Phone Code: 123
- Start Time: 29th November 2008 (midnight)
- EndTime: 30th November 2008 (midnight)
- Timezone: Europe/London
- Time Profile: StartEnd (as created in the time profile user interface)

2. Call the API as follows:

<http://x.x.x.x/sponsor/api/GuestAccount.php?username=local&password=local&method=create&firstName=John&surname=Carter&email=johncart@merunetworks.com&role=DEFAULT&company=Meru&mobileNumber=12345+48434532&phoneCode=-11-29&endTime=2008-11-30&timezone=Europe%2FLondon&timeProfile=StartEnd>

3. If successful, a response is returned:

```
<?xml version="1.0"?>
```



```

<response>
  <status>
    <code>0</code>
    <message>Success</message>
  </status>
  <account/>
  <account>
    <id>815</id>
    <firstName>John</firstName>
    <surname>Carter</surname>
    <company>Fortinet</company>
    <email>johncart@merunetworks.com</email>
    <mobileNumber>12345 48434532</mobileNumber>
    <phoneCode>123</phoneCode>
    <option1/>
    <option2/>
    <option3/>
    <option4/>
    <option5/>
    <username>JohnCarter10</username>
    <password>!B,4N!32(F1{VJ2</password>
    <status>1</status>
    <bulkId/>
    <timezone>Europe/London</timezone>
    <startTimeT>2008-11-29T00:00:00+00:00</startTimeT>
    <endTimeT>2008-11-30T00:00:00+00:00</endTimeT>
    <role/>
    <createdTime/>
    <modifiedUsername>1</modifiedUsername>

```

```
<timeProfile>
  <id>2</id>
  <name>StartEnd</name>
  <description/>
  <duration>0</duration>
  <accountType>1</accountType>
  <durationUnit>Days</durationUnit>
  <durationInUnits>0</durationInUnits>
  <restriction>
    <id>43</id>
    <weekDay>1</weekDay>
    <startTime>00:00</startTime>
    <endTime>08:59</endTime>
  </restriction>
  <restriction>
    <id>45</id>
    <weekDay>3</weekDay>
    <startTime>00:00</startTime>
    <endTime>08:59</endTime>
  </restriction>
  <restriction>
    <id>50</id>
    <weekDay>3</weekDay>
    <startTime>17:00</startTime>
    <endTime>23:59</endTime>
  </restriction>
  <restriction>
    <id>51</id>
    <weekDay>4</weekDay>
```

```

        <startTime>17:00</startTime>
        <endTime>23:59</endTime>
    </restriction>
    <restriction>
        <id>47</id>
        <weekDay>5</weekDay>
        <startTime>00:00</startTime>
        <endTime>08:59</endTime>
    </restriction>
    <restriction>
        <id>54</id>
        <weekDay>7</weekDay>
        <startTime>00:00</startTime>
        <endTime>23:59</endTime>
    </restriction>
</timeProfile>
</account>
</response>

```

edit

The edit method edits an existing user account in accordance with sponsor's permissions.

You may edit any of the fields associated with an existing account with the following exceptions:

- start time
- role
- time profile
- time zone

To edit an account, you must supply the account ID as returned by the create method.

Required In Parameters

- method (required): edit
- id (required): The database ID of the account to be edited
- username (required): Sponsor account username
- password (required): Sponsor account password
- firstName (optional): Guest user first name
- surname (optional): Guest user surname
- email (optional): Guest user email address
- group (optional): The role in which the guest user is created
- company (optional): Guest user company name
- phonecode (optional): Telephone code for the Guest user mobile telephone (e.g. +44)
- cellnumber (optional): Cell telephone number for the Guest user
- timezone (optional): The timezone in which the guest account is created (as detailed in Valid Timezones)
- option1 (optional): Optional data field 1
- option2 (optional): Optional data field 2
- option3 (optional): Optional data field 3
- option4 (optional): Optional data field 4
- option5 (optional): Optional data field 5
- startTime (optional): The time the account is due to start
- endTime (optional): The time the account should end
- timeProfile (optional): The time profiler to use when creating the account

edit Example Use

The following example changes the mobile phone (cell phone) number for the account with ID 794:

<http://x.x.x.x/sponsor/api/GuestAccount.php?username=local&password=local&method=edit&id=794&mobileNumber=12345678>

The full account detail is returned as with the getDetails method.

```
<?xml version="1.0"?>
<response>
  <status>
```

```

<code>0</code>

<message>Success</message>
</status>
<account/>
<account>
  <id>794</id>
  <firstName>John</firstName>
  <surname>Carter</surname>
  <company>Fortinet</company>
  <email>johncart@merunetworks.com</email>
  <mobileNumber>12345678</mobileNumber>
  <phoneCode>123</phoneCode>
  <option1>1</option1>
  <option2>1</option2>
  <option3>1</option3>
  <option4>1</option4>
  <option5>1</option5>
  <username>jcarter</username>
  <password>Fortinet</password>
  <status>1</status>
  <bulkId/>
  <timezone>Europe/London</timezone>
  <startTimeT>2008-10-28T00:00:00+00:00</startTimeT>
  <endTimeT>2008-10-29T00:00:00+00:00</endTimeT>
  <role/>
  <createdTime/>
  <modifiedUsername/>
  <usage>
    <startTime>2008-08-07T04:06:32+01:00</startTime>

```

```

    <endTime>2008-08-07T04:06:33+01:00</endTime>
    <ipAddress>4.5.6.7</ipAddress>
</usage>
<usage>
    <startTime>2008-10-02T22:00:00+01:00</startTime>
    <endTime>2008-10-03T00:30:00+01:00</endTime>
    <ipAddress>4.5.6.7</ipAddress>
</usage>
<timeProfile>
    <id>2</id>
    <name>StartEnd</name>
    <description/>
    <duration>0</duration>
    <accountType>1</accountType>
    <durationUnit>Days</durationUnit>
    <durationInUnits>0</durationInUnits>
    <restriction>
        <id>43</id>
        <weekDay>1</weekDay>
        <startTime>00:00</startTime>
        <endTime>08:59</endTime>
    </restriction>
    <restriction>
        <id>45</id>
        <weekDay>3</weekDay>
        <startTime>00:00</startTime>
        <endTime>08:59</endTime>
    </restriction>
    <restriction>

```

```
<id>50</id>
<weekDay>3</weekDay>
<startTime>17:00</startTime>
<endTime>23:59</endTime>
</restriction>
<restriction>
  <id>51</id>
  <weekDay>4</weekDay>
  <startTime>17:00</startTime>
  <endTime>23:59</endTime>
</restriction>
<restriction>
  <id>47</id>
  <weekDay>5</weekDay>
  <startTime>00:00</startTime>
  <endTime>08:59</endTime>
</restriction>
<restriction>
  <id>54</id>
  <weekDay>7</weekDay>
  <startTime>00:00</startTime>
  <endTime>23:59</endTime>
</restriction>
</timeProfile>
</account>
</response>
```

getDetails

The getDetails API gets a user's account details in accordance with the sponsor's permissions.

Required In Parameters

- method (required): getDetails
- username (required): Sponsor account username
- password (required): Sponsor account password
- id (one required): ID of the account to be retrieved

getDetails Example Use

1. To get details for an existing account, use the getDetails API call, passing in the ID of the account as returned by the create method:

<http://x.x.x.x/sponsor/api/GuestAccount.php?username=local&password=local&method=getDetails&id=815>

2. If successful the following response will be returned:

```
<?xml version="1.0"?>
<response>
  <status>
    <code>0</code>
    <message>Success</message>
  </status>
  <account/>
  <account>
    <id>815</id>
    <firstName>John</firstName>
    <surname>Carter</surname>
    <company>Fortinet</company>
```



```

<email>johncart@merunetworks.com</email>
<mobileNumber>12345 48434532</mobileNumber>
<phoneCode>123</phoneCode>
<option1>aaa</option1>
<option2>bbb</option2>
<option3/>
<option4>ddd</option4>
<option5>eee</option5>
<username>jcarter</username>
<password>*****</password>
<status>1</status>
  <bulkId/>
  <timezone>Europe/London</timezone>
  <startTimeT>2008-10-29T00:00:00+00:00</startTimeT>
  <endTimeT>2008-10-30T00:00:00+00:00</endTimeT>
  <role/>
  <createdTime/>
  <modifiedUsername/>
  <usage>
    <startTime>2008-08-07T04:06:32+01:00</startTime>
    <endTime>2008-08-07T04:06:33+01:00</endTime>
    <ipAddress>4.5.6.7</ipAddress>
  </usage>
  <usage>
    <startTime>2008-10-02T22:00:00+01:00</startTime>
    <endTime>2008-10-03T00:30:00+01:00</endTime>
    <ipAddress>4.5.6.7</ipAddress>
  </usage>
  <timeProfile>

```

```
<id>2</id>
<name>StartEnd</name>
<description/>
<duration>0</duration>
<accountType>1</accountType>
<durationUnit>Days</durationUnit>
<durationInUnits>0</durationInUnits>
<restriction>
  <id>43</id>
  <weekDay>1</weekDay>
  <startTime>00:00</startTime>
  <endTime>08:59</endTime>
</restriction>
<restriction>
  <id>45</id>
  <weekDay>3</weekDay>
  <startTime>00:00</startTime>
  <endTime>08:59</endTime>
</restriction>
<restriction>
  <id>50</id>
  <weekDay>3</weekDay>
  <startTime>17:00</startTime>
  <endTime>23:59</endTime>
</restriction>
<restriction>
  <id>51</id>
  <weekDay>4</weekDay>
  <startTime>17:00</startTime>
```

```

        <endTime>23:59</endTime>
    </restriction>
    <restriction>
        <id>47</id>
        <weekDay>5</weekDay>
        <startTime>00:00</startTime>
        <endTime>08:59</endTime>
    </restriction>
    <restriction>
        <id>54</id>
        <weekDay>7</weekDay>
        <startTime>00:00</startTime>
        <endTime>23:59</endTime>
    </restriction>
</timeProfile>
</account>
</response>

```

suspend

The suspend method suspends a user account in accordance with sponsor's permissions.

Required In Parameters

- method (required): suspend
- username (required): Sponsor account username
- password (required): Sponsor account password
- id (required): The database ID of the account to be suspended

suspend Example Use

The suspend method suspends the account and returns the same XML response as getDetails.

<http://x.x.x.x/sponsor/api/GuestAccount.php?username=local&password=local&method=suspend&&&id=815>

notifyEmail

The notifyEmail method sends an email message to the guest's email account. It returns the same XML as getDetails.

- Required In Parameters
- method (required): notifyEmail
- username (required): Sponsor account username
- password (required): Sponsor account password
- id (required): The database ID of the account to be emailed
- from (required): The email address from which to send the email
- to (required): the email address to send the email to

notifyEmail Example Use

<http://x.x.x.x/sponsor/api/GuestAccount.php?username=local&password=local&method=notifyEmail.&&&id=815>.

notifySMS

The notifySms method sends an SMS message to the guest's mobile (cell) phone. It returns the same XML as getDetails.

Required In Parameters

- method (required): notifySms

- username (required): Sponsor account username
- password (required): Sponsor account password
- id (required): The database ID of the account to be emailed

notifySMS Example Use

<http://x.x.x.x/sponsor/api/GuestAccount.php?username=local&password=local&method=notifySms&&&&id=815>.

getVersion

The getVersion method shows the current API version.

Required In Parameters

- method (required): getVersion
- username (required): Sponsor account username
- password (required): Sponsor account password

getVersion Example Use

A call return a response of the form:

```
<?xml version="1.0"?>
<response>
  <status>
    <code>0</code>
    <message>Success</message>
  </status>
  <appName>Cisco NAC Guest Server</appName>
```

search

```
<version>2.0.2</version>
<majorVersion>2</majorVersion>
<minorVersion>0</minorVersion>
<maintenanceVersion>2</maintenanceVersion>
</response>
```

search

The search API returns guest account details for reporting purposes according to the sponsor's permissions and configuration, as per the Managing Guest Accounts of the sponsor interface.

Required In Parameters

- username (required): sponsor account username
- password (required): sponsor account password
- method (required): search
- sponsor (optional): sponsor username
- guestUsername (optional): guest username
- firstName (optional): guest user first name
- surname (optional): guest user surname
- company (optional): guest user company name
- email (optional): guest user email address
- ipAddress (optional)
- startTime (optional): YYYY-MM-DD
- endTime (optional): YYYY-MM-DD
- timezone (optional): Timezone in which the account is create
- timeProfile (optional): time profile name
- accountGroup - name of account group (string)
- mobileNumber (optional): guest mobile number
- phoneCode (optional): guest mobile number country code
- guestPortal (optional): guest portal name used by the guest to self register his account
- option1 (optional):
- option2 (optional):
- option3 (optional):

- option4 (optional):
- option5 (optional):
- statusInactive (optional):
- statusActive (optional):
- statusExpired (optional):
- statusSuspended (optional):
- statusPending (optional):
- statusRejected (optional):

search Example Use

The required parameters are mandatory. The optional parameters serve to subset the data returned. If the start and end date are not specified, then accounts spanning the last 24 hours are returned.

The following example returns details of active guest accounts between 3rd March 2009 and 15th April 2009.

<http://x.x.x.x/sponsor/api/GuestAccount.php?username=local&password=local&method=search&startTime=2009-03-03&endTime=2009-04-15&statusActive=1>

If successful, the following response will be returned.

```
<response>

  <status>

    <code>0</code>

    <message>Success</message>

  </status>

  <item>

    <id>2005</id>

    <firstName>Jim</firstName>

    <surname>Bean</surname>

    <company>Beans Brewery</company>

    <email>jim@bean.com</email>

    <username> jim@bean.com </username>

    <password>Es3TDdd3</password>
```

search Example Use

```
<status>2</status>
<mobileNumber>782394928</mobileNumber>
<phoneCode>1</phoneCode>
<timezone>America/Los_Angeles</timezone>
<option1/>
<option2/>
<option3/>
<option4/>
<option5/>
<startTimeT>2009-04-01T04:40:00+00:00</startTimeT>
<endTimeT>2009-04-06T06:59:00+00:00</endTimeT>
<role>Default</role>
<sponsorId>196</sponsorId>
<sponsor>sam</sponsor>
<timeProfileId>1</timeProfileId>
<timeProfile>default</timeProfile>
</item>
<item>
  ...further account details meeting the request criteria...
</item>
<item>
  ...further account details meeting the request criteria...
</item>
<item>
  ...further account details meeting the request criteria...
</item>
</response>
```


approve

Approves a guest account

Note: The approve API is only available from Versions 10.11 and later. Required in parameters are :

- method (required) : approve
- id (required) : id for the guest account
- username (required) : username for the sponsor making the API call
- password (required) : password for the sponsor making the API call

approve example use

Approve example input method:

`http://10.53.0.244/sponsor/api/GuestAccount.php?`

`username=local&password=local&method=approve&id=1`

```
<?xml version="1.0"?>
```

```
<response>
```

```
  <status>
```

```
    <code>0</code>
```

```
    <message>Success</message>
```

```
  </status>
```

```
  <account>
```

```
    <username>test@test.com</username>
```

```
    <password>a</password>
```

```
    <failedLoginAttempts>0</failedLoginAttempts>
```

```
    <modifiedUsername/>
```

```
    <lastMonitoredLogRefresh/>
```

```
    <duration/>
```

```
    <allowedWindow/>
```

approve example use

```
<approvalDecisionDate>2010-11-18T10:20:46-05:00</approvalDecisionDate>
  <eventCode>
    <id/>
    <sponsor/>
    <startTime/>
    <endTime/>
    <timezone/>
    <maxAccounts>0</maxAccounts>
    <code/>
    <status>1</status>
    <description/>
    <timeProfile/>
    <guestRole/>
  </eventCode>
  <approvalRequestEmail/>
  <nextApprovalNotification/>
  <rejectReason/>
  <id>1</id>
  <firstName>test</firstName>
  <surname>test</surname>
  <company>test</company>
  <email>test@test.com</email>
  <mobileNumber/>
  <phoneCode/>
  <option1/>
  <option2/>
  <option3/>
  <option4/>
  <option5/>
```

```

<status>1</status>

<bulkId/>

<timezone>America/Lima</timezone>

<startTimeT>2010-11-18T10:18:00-05:00</startTimeT>

<endTimeT>2010-11-18T23:59:00-05:00</endTimeT>

<role>

  <id>3</id>

  <name>Default</name>

  <description>Default Role</description>

  <maxConcurrentConnections>0</maxConcurrentConnections>

  <maxFailedAuthAttempts>2</maxFailedAuthAttempts>

  <allowPasswordChange/>

  <requirePasswordChange/>

  <passwordChangeInterval/>

</role>

<createdTime>2010-11-18T15:18:53+00:00</createdTime>

<hotspot/>

<restricted/>

<timeProfile>

  <id>1</id>

  <name>default</name>

  <description>Default time profile</description>

  <duration/>

  <timezone/>

  <accountType>1</accountType>

  <durationUnit>D</durationUnit>

  <durationInUnits>0</durationInUnits>

  <allowedWindow/>

  <windowUnit>D</windowUnit>

```

disableRememberMe

```
<windowInUnits>0</windowInUnits>  
</timeProfile>  
</account>  
</response>
```

disableRememberMe

Disables remember me option of a guest till it is enabled again by the guest. Remember me can be disabled either using guest user id or Mac Address.

Required parameters

method (required): disableRememberMe

username (required): Sponsor account username

password (required): Sponsor account password

id (required): The database ID of the account to be suspended or MAC Address

disableRememberMe Example Use

The disableRememberMe method deletes the data used by remember me feature and forces guest user to explicitly login during his next visit.

API returns the same XML response as getDetails.

<http://x.x.x.x/sponsor/api/GuestAccount.php?username=local&password=local6&method=disableRememberMe&id=2815>

reject

Rejects a guest account

Note: The reject API is only available from Versions 10.11 and later. Required in parameters are:

- method (required) : reject
- id (required) : id for the guest account

- username (required) : username for the sponsor making the API call password (required) : password for the sponsor making the API call

reject example use

Reject example input:

`http://10.53.0.244/sponsor/api/GuestAccount.php?`

`username=local&password=local&method=reject&id=1`

```
<?xml version="1.0"?>
<response>
  <status>
    <code>0</code>
    <message>Success</message>
  </status>
  <account>
    <username>test@test.com</username>
    <password>a</password>
    <failedLoginAttempts>0</failedLoginAttempts>
    <modifiedUsername/>
    <lastMonitoredLogRefresh/>
    <duration/>
    <allowedWindow/>
  </account>
  <approvalDecisionDate>2010-11-18T10:22:52-05:00</approvalDecisionDate>
  <eventCode>
    <id/>
    <sponsor/>
    <startTime/>
    <endTime/>
    <timezone/>
  </eventCode>
</response>
```

reject example use

```
<maxAccounts>0</maxAccounts>

<code/>

<status>1</status>

<description/>

<timeProfile/>

<guestRole/>

</eventCode>

<approvalRequestEmail/>

<nextApprovalNotification/>

<rejectReason/>

<id>1</id>

<firstName>test</firstName>

<surname>test</surname>

<company>test</company>

<email>test@test.com</email>

<mobileNumber/>

<phoneCode/>

<option1/>

<option2/>

<option3/>

<option4/>

<option5/>

<status>6</status>

<bulkId/>

<timezone>America/Lima</timezone>

<startTimeT>2010-11-18T10:18:00-05:00</startTimeT>

<endTimeT>2010-11-18T23:59:00-05:00</endTimeT>

<role>

  <id>3</id>
```

```

    <name>Default</name>
    <description>Default Role</description>
    <maxConcurrentConnections>0</maxConcurrentConnections>
    <maxFailedAuthAttempts>2</maxFailedAuthAttempts>
    <allowPasswordChange/>
    <requirePasswordChange/>
    <passwordChangeInterval/>
  </role>
  <createTime>2010-11-18T15:18:53+00:00</createTime>
  <hotspot/>
  <restricted/>
  <timeProfile>
    <id>1</id>
    <name>default</name>
    <description>Default time profile</description>
    <duration/>
    <timezone/>
    <accountType>1</accountType>
    <durationUnit>D</durationUnit>
    <durationInUnits>0</durationInUnits>
    <allowedWindow/>
    <windowUnit>D</windowUnit>
    <windowInUnits>0</windowInUnits>
  </timeProfile>
</account>
</response>

```

Device Account API

CreateDevice

The createDevice method creates a device account in accordance with the sponsor's permissions.

Usage:

Required In Parameters

method (required): createDevice

username (required): Sponsor account username

password (required): Sponsor account password

macAddress

(required): Sponsor account username

firstName (based on policy): user first name

surname (based on policy): user surname

company (based on policy): Guest user company name

email (based on policy): Guest user email address

phonecode (based on policy): Telephone code for the Guest user mobile telephone (e.g. +44)

mobilenumber (based on policy): Mobile telephone number for the Guest user

accountGroup - name of account group (string)

timeProfile (required): The time profile to use when creating the account

timezone (required): Timezone in which the account is created (as per Valid Timezones, page A-13)

startTime (required): The time the account is due to start

endTime (required): The time the account should end

option1 (based on policy): Optional data field 1

option2 (based on policy): Optional data field 2

option3 (based on policy): Optional data field 3

option4 (based on policy): Optional data field 4

option5 (based on policy): Optional data field 5

createDevice Example:

The following example creates a device account with the details below:

Mac Address: 12-12-78-3b-cd-25
 First Name: samuel
 Surname: samuel
 Company: Fortinet
 Email: samuel@Fortinet.com
 Phone Code: 44
 Mobile Number (cellphone):
 07929379212
 Role: Default
 Time Profile: Default
 Timezone: Europe/London
 Start Time: 16th March 2012 (midnight)
 EndTime: 16th April 2012 (midnight)

Call the API as follows:

<http://x.x.x.x/sponsor/api/GuestAccount.php?username=xxx&password=xxx&method=createDevice&macAddress=12-12-78-3b-cd-255&firstName=samuel&surname=samuel&company=meru&email=sam@meru.com&phoneCode=44&mobileNumber=07929379212&role=Default&timeProfile=Default&timezone=Europe%2FLondon&startTime=2012-03-16&endTime=2012-04-16>

If successful, a response is returned in the form:

```

<?xml version="1.0"?>
<response>
  <status>
    <code>0</code>
    <message>Success</message>
  </status>
  <account>
    <macAddress>12-12-78-3b-cd-25</macAddress>
    <startTime>2012-03-16T00:00:00+00:00</startTime>
    <endTime>2012-04-16T00:00:00+01:00</endTime>
    <id>1</id>
    <firstName>samuel</firstName>
    <surname>samuel</surname>
    <company>meru</company>
    <email>samuel@meru.com</email>
  </account>
</response>
  
```

```

<mobileNumber>07929379212</mobileNumber>
<phoneCode>44</phoneCode>
<option1/>
<option2/>
<option3/>
<option4/>
<option5/>
<status>1</status>
<bulkId/>
<timezone>Europe/London</timezone>
<startTimeT>2012-03-16T00:00:00+00:00</startTimeT>
<endTimeT>2012-04-16T00:00:00+01:00</endTimeT>
<createdTime>2012-03-16T03:47:48-07:00</createdTime>
<restricted/>
<timeProfile>
  <id>1</id>
  <name>default</name>
  <description>Default time profile</description>
  <duration/>
  <timezone/>
  <accountType>1</accountType>
  <durationUnit>D</durationUnit>
  <durationInUnits>0</durationInUnits>
  <allowedWindow/>
  <windowUnit>D</windowUnit>
  <windowInUnits>0</windowInUnits>
</timeProfile>
</account>
</response>

```

editDevice

The editDevice method edits an existing device account in accordance with sponsor's permissions. To edit an account, you must supply the account ID as returned by createDevice above.

Usage:

Required In Parameters

method (required): editDevice
 username (required): Sponsor account username
 password (required): Sponsor account password
 id (required): The database ID of the device account to be edited
 firstName (optional): Guest user first name
 surname (optional): Guest user surname
 email (optional): Guest user email address
 group (optional): The role in which the guest user is created
 company (optional): Guest user company name
 phonecode (optional): Telephone code for the Guest user mobile telephone (e.g. +44)
 cellnumber (optional): Cell telephone number for the Guest user
 timezone (optional): The timezone in which the guest account is created (as per Valid Timezones)
 option1 (optional): Optional data field 1
 option2 (optional): Optional data field 2
 option3 (optional): Optional data field 3
 option4 (optional): Optional data field 4
 option5 (optional): Optional data field 5
 startTime (optional): The time the account is due to start
 endTime (optional): The time the account should end
 timeProfile (optional): The time profiler to use when creating the account

editDevice Example:

The following example changes mobile / cell phone number & end date for an account with ID 1:

<http://x.x.x.x/sponsor/api/GuestAccount.php?username=xxx&password=xxx&method=editDevice&id=1&mobileNumber=0794122222&endTime=2012-07-09>

The full account detail are returned:-

```

<?xml version="1.0"?>
<response>
  <status>
    <code>0</code>
    <message>Success</message>
  </status>
  <account>

```

```

<macAddress>12-12-78-3B-CD-23</macAddress>
<startTime>2012-03-16T00:00:00+00:00</startTime>
<endTime>2012-07-09T00:00:00-07:00</endTime>
<id>1</id>
<firstName>samuel</firstName>
<surname>samuel</surname>
<company>meru</company>
<email>samuel@meru.com</email>
<mobileNumber>07941222222</mobileNumber>
<phoneCode>44</phoneCode>
<option1/>
<option2/>
<option3/>
<option4/>
<option5/>
<bulkId/>
<timezone>Europe/London</timezone>
<startTimeT>2012-03-16T00:00:00+00:00</startTimeT>
<endTimeT>2012-07-09T00:00:00-07:00</endTimeT>
<createdTime>2012-03-16T10:47:48+00:00</createdTime>
<restricted/>
<timeProfile>
  <id>1</id>
  <name>default</name>
  <description>Default time profile</description>
  <duration/>
  <timezone/>
  <accountType>1</accountType>
  <durationUnit>D</durationUnit>
  <durationInUnits>0</durationInUnits>
  <allowedWindow/>
  <windowUnit>D</windowUnit>
  <windowInUnits>0</windowInUnits>
  <restrictions/>
</timeProfile>
</account>
</response>

```

getDeviceDetails

The getDeviceDetails retrieves device account details in accordance with the sponsor's permissions.

Usage:

Required In Parameters

method (required): getDeviceDetails

username (required): Sponsor account username

password (required): Sponsor account password

id (required): ID of the account to be retrieved

getDeviceDetails Example

To fetch details of an existing device account using the ID of the account as returned by createDevice:

`http://x.x.x.x/sponsor/api/GuestAccount.php?username=xxx&password=xxx&method=getDeviceDetails&id=1`

The full account detail are returned:-

```

<?xml version="1.0"?>
<response>
  <status>
    <code>0</code>
    <message>Success</message>
  </status>
  <account>
    <macAddress>12-12-78-3B-CD-23</macAddress>
    <startTime>2012-03-16T00:00:00+00:00</startTime>
    <endTime>2012-07-09T08:00:00+01:00</endTime>
    <id>1</id>
    <firstName>samuel</firstName>
    <surname>samuel</surname>
    <company>meru</company>
    <email>samuel@meru.com</email>
    <mobileNumber>07941222222</mobileNumber>
  </account>
</response>

```

```

<phoneCode>44</phoneCode>
<option1/>
<option2/>
<option3/>
<option4/>
<option5/>
<status>2</status>
<bulkId/>
<timezone>Europe/London</timezone>
<startTimeT>2012-03-16T00:00:00+00:00</startTimeT>
<endTimeT>2012-07-09T08:00:00+01:00</endTimeT>
<createdTime>2012-03-16T10:47:48+00:00</createdTime>
<restricted/>
<timeProfile>
  <id>1</id>
  <name>default</name>
  <description>Default time profile</description>
  <duration/>
  <timezone/>
  <accountType>1</accountType>
  <durationUnit>D</durationUnit>
  <durationInUnits>0</durationInUnits>
  <allowedWindow/>
  <windowUnit>D</windowUnit>
  <windowInUnits>0</windowInUnits>
  <restrictions/>
</timeProfile>
</account>
</response>

```

suspend

Device

The suspendDevice method suspends a device account in accordance with sponsor's permissions.

Usage:

Required In Parameters

method (required): suspendDevice
username (required): Sponsor account username
password (required): Sponsor account password
id (required): ID of the device account to be suspended

suspendDevice Example

The suspendDevice method suspends the account & returns the same XML response as getDeviceDetails.

<http://x.x.x.x/sponsor/api/GuestAccount.php?username=xxx&password=xxx&method=suspendDevice&id=1>

deviceNotifyEmail

The deviceNotifyEmail method sends an email message to the device accounts email address & returns the same XML response as getDeviceDetails.

Usage:

Required In Parameters

method (required): deviceNotifyEmail
username (required): Sponsor account username
password (required): Sponsor account password
id (required): ID of the device account to be emailed

deviceNotifyEmail Example

<http://x.x.x.x/sponsor/api/GuestAccount.php?username=xxx&password=xxx&method=deviceNotifyEmail.&id=1>

deviceNotifySms

The deviceNotifySms method sends an SMS message to the account mobile / cell phone & returns the same XML response as getDeviceDetails.

Usage:

Required In Parameters

method (required): notifySms
username (required): Sponsor account username
password (required): Sponsor account password
id (required): The ID of the account to be messaged via SMS

deviceNotifySms Example Use

<http://x.x.x.x/sponsor/api/GuestAccount.php?username=xxx&password=xxx&method=deviceNotifySms&id=1>

searchDevices

The searchDevices API call returns device account details for reporting purposes according to the sponsor's permissions.

Usage:

Required In Parameters

method (required): searchDevices
username (required): Sponsor account username
password (required): Sponsor account password
id (required): The ID of the account to be messaged via SMS
sponsor (optional): sponsor username
macAddress (optional): guest username

firstName (optional): account first name
 surname (optional): account surname
 company (optional): account company name
 email (optional): account email address
 ipAddress (optional)
 startTime (optional): YYYY-MM-DD
 endTime (optional): YYYY-MM-DD
 timezone (optional): Timezone in which the account is create
 timeProfile (optional): time profile name
 accountGroup - name of account group (string)
 mobileNumber (optional): guest mobile number
 phoneCode (optional): guest mobile number country code
 guestPortal (optional): guest portal name used by the guest to self register his account
 option1 (optional):
 option2 (optional):
 option3 (optional):
 option4 (optional):
 option5 (optional):
 statusInactive (optional):
 statusActive (optional):
 statusExpired (optional):
 statusSuspended (optional):

searchDevices Example

Optional parameters serve to subset the data returned. If the start and end date are not specified then only accounts spanning the last 24 hours are returned.

The following example returns details of active device accounts between 1st January 2012 and 31st December 2012.

`http://x.x.x.x/sponsor/api/GuestAccount.php?username=xxx&password=xxx&method=searchDevices&startTime=2012-01-01&endTime=2012-12-31&statusActive=1`

On success, the following response will be returned.

```
<?xml version="1.0"?>
```

```

<response>
  <status>
    <code>0</code>
    <message>Success</message>
  </status>
  <item>
    <id>1</id>
    <macaddress>12:12:78:3B:CD:23</macaddress>
    <firstName>samuel</firstName>
    <surname>samuel</surname>
    <company>meru</company>
    <email>samuel@meru.com</email>
    <status>2</status>
    <mobileNumber>07941222222</mobileNumber>
    <phoneCode>44</phoneCode>
    <timezone>Europe/London</timezone>
    <option1/>
    <option2/>
    <option3/>
    <option4/>
    <option5/>
    <startTime>2012-03-16T00:00:00+00:00</startTime>
    <endTime>2012-07-09T07:00:00+00:00</endTime>
    <role>Default</role>
    <sponsorId>196</sponsorId>
    <sponsor>Sam</sponsor>
    <timeProfileId>1</timeProfileId>
    <timeProfile>default</timeProfile>
  </item>
  <item>
    <id>2</id>
    <macaddress>BB:1C:7C:3B:CD:24</macaddress>
    <firstName>John</firstName>
    <surname>James</surname>
    <company>meru</company>
    <email>jj@merunetworks.com</email>
    <status>2</status>
    <mobileNumber>07929379212</mobileNumber>
    <phoneCode>44</phoneCode>
    <timezone>Europe/London</timezone>

```

```

<option1/>
<option2/>
<option3/>
<option4/>
<option5/>
<startTime>2012-01-16T00:00:00+00:00</startTime>
<endTime>2012-08-15T23:00:00+00:00</endTime>
<role>Default</role>
<sponsorId>192</sponsorId>
<sponsor>Will</sponsor>
<timeProfileId>1</timeProfileId>
<timeProfile>default</timeProfile>
</item>

<item>
...further account details meeting the request criteria...
</item>

<item>
...further account details meeting the request criteria...
</item>

<item>
...further account details meeting the request criteria...
</item>

</response>

```

Status Codes

The account status is returned via XML and contains the following values:

- Status inactive = 1
- Status active = 2
- Status expired = 3
- Status suspended = 4

Error Codes

The following error codes are returned in the <code> element of the response. Value - Description:

- Value 0—No error
- Value 1—Internal application error
- Value 100—Incorrect sponsor username and/or password
- Value101—Cannot access API via HTTPS (controlled by administrator)
- Value102—Cannot access API via HTTP (controlled by administrator)
- Value 1000—Some required fields are missing (listed in the message)
- Value1001—Sending SMS messages disabled by administrator
- Value1002—Sending Emails disabled by administrator
- Value1003—The passed account ID does not exist
- Value1004—Some fields are incorrect (listed in the message)
- Value 1005—Some fields cannot be changed using the edit method

Valid Timezones

Africa/Abidjan Africa/Accra Africa/Addis_Ababa Africa/Algiers Africa/Asmara Africa/Bamako
 Africa/Bangui Africa/Banjul Africa/Bissau Africa/Blantyre Africa/Brazzaville Africa/Bujumbura
 Africa/Cairo Africa/Casablanca Africa/Ceuta Africa/Conakry Africa/Dakar Africa/Dar_es_Salaam
 Africa/Djibouti Africa/Douala Africa/El_Aaiun Africa/Freetown Africa/Gaborone Africa/Harare
 Africa/Johannesburg Africa/Kampala Africa/Khartoum Africa/Kigali Africa/Kinshasa Africa/Lagos
 Africa/Libreville Africa/Lome Africa/Luanda Africa/Lubumbashi Africa/Lusaka Africa/Malabo
 Africa/Maputo Africa/Maseru Africa/Mbabane Africa/Mogadishu Africa/Monrovia Africa/Nairobi
 Africa/Ndjamena Africa/Niamey Africa/Nouakchott Africa/Ouagadougou Africa/Porto-Novo
 Africa/Sao_Tome Africa/Tripoli Africa/Tunis Africa/Windhoek America/Adak America/Anchorage
 America/Anguilla America/Antigua America/Araguaina America/Argentina/Buenos_Aires
 America/Argentina/Catamarca America/Argentina/Cordoba America/Argentina/Jujuy
 America/Argentina/La_Rioja America/Argentina/Mendoza America/Argentina/Rio_Gallegos
 America/Argentina/San_Juan America/Argentina/Tucuman America/Argentina/Ushuaia America/Aruba
 America/Asuncion America/Atikokan America/Bahia America/Barbados America/Belem America/Belize
 America/Blanc-Sablon America/Boa_Vista America/Bogota America/Boise America/Cambridge_Bay
 America/Campo_Grande America/Cancun America/Caracas America/Cayenne America/Cayman
 America/Chicago America/Chihuahua America/Costa_Rica America/Cuiaba America/Curacao
 America/Danmarkshavn America/Dawson America/Dawson_Creek America/Denver America/Detroit
 America/Dominica America/Edmonton America/Eirunepe America/El_Salvador America/Fortaleza
 America/Glace_Bay America/Godthab America/Goose_Bay America/Grand_Turk America/Grenada
 America/Guadeloupe America/Guatemala America/Guayaquil America/Guyana America/Halifax
 America/Havana America/Hermosillo America/Indiana/Indianapolis America/Indiana/Knox

America/Indiana/Marengo America/Indiana/Petersburg America/Indiana/Tell_City
 America/Indiana/Vevay America/Indiana/Vincennes America/Indiana/Winamac America/Inuvik
 America/Iqaluit America/Jamaica America/Juneau America/Kentucky/Louisville
 America/Kentucky/Monticello America/La_Paz America/Lima America/Los_Angeles America/Maceio
 America/Managua America/Manaus America/Martinique America/Mazatlan America/Menominee
 America/Merida America/Mexico_City America/Miquelon America/Moncton America/Monterrey
 America/Montevideo America/Montreal America/Montserrat America/Nassau
 America/New_York America/Nipigon America/Nome America/Noronha America/North_Dakota/Center
 America/North_Dakota/New_Salem America/Panama America/Pangnirtung America/Paramaribo
 America/Phoenix America/Port-au-Prince America/Port_of_Spain America/Porto_Velho
 America/Puerto_Rico America/Rainy_River America/Rankin_Inlet America/Recife America/Regina
 America/Resolute America/Rio_Branco America/Santiago America/Santo_Domingo America/Sao_Paulo
 America/Scoresbysund America/Shiprock America/St_Johns America/St_Kitts America/St_Lucia
 America/St_Thomas America/St_Vincent America/Swift_Current America/Tegucigalpa America/Thule
 America/Thunder_Bay America/Tijuana America/Toronto America/Tortola America/Vancouver
 America/Whitehorse America/Winnipeg America/Yakutat America/Yellowknife Antarctica/Casey
 Antarctica/Davis Antarctica/DumontDUrville Antarctica/Mawson Antarctica/McMurdo
 Antarctica/Palmer Antarctica/Rothera Antarctica/South_Pole Antarctica/Syowa Antarctica/Vostok
 Arctic/Longyearbyen Asia/Aden Asia/Almaty Asia/Amman Asia/Anadyr Asia/Aqtou Asia/Aqtobe
 Asia/Ashgabat Asia/Baghdad Asia/Bahrain Asia/Baku Asia/Bangkok Asia/Beirut Asia/Bishkek
 Asia/Brunei Asia/Calcutta Asia/Choibalsan Asia/Chongqing Asia/Colombo Asia/Damascus Asia/Dhaka
 Asia/Dili Asia/Dubai Asia/Dushanbe Asia/Gaza Asia/Harbin Asia/Hong_Kong Asia/Hovd Asia/Irkutsk
 Asia/Jakarta Asia/Jayapura Asia/Jerusalem Asia/Kabul Asia/Kamchatka Asia/Karachi Asia/Kashgar
 Asia/Katmandu Asia/Krasnoyarsk Asia/Kuala_Lumpur Asia/Kuching Asia/Kuwait Asia/Macau
 Asia/Magadan Asia/Makassar Asia/Manila Asia/Muscat Asia/Nicosia Asia/Novosibirsk Asia/Omsk
 Asia/Oral Asia/Phnom_Penh Asia/Pontianak Asia/Pyongyang Asia/Qatar Asia/Qyzylorda Asia/Rangoon
 Asia/Riyadh Asia/Saigon Asia/Sakhalin Asia/Samarkand Asia/Seoul Asia/Shanghai Asia/Singapore
 Asia/Taipei Asia/Tashkent Asia/Tbilisi Asia/Tehran Asia/Thimphu Asia/Tokyo Asia/Ulaanbaatar
 Asia/Urumqi Asia/Vientiane Asia/Vladivostok Asia/Yakutsk Asia/Yekaterinburg Asia/Yerevan
 Atlantic/Azores Atlantic/Bermuda Atlantic/Canary Atlantic/Cape_Verde Atlantic/Faroe
 Atlantic/Jan_Mayen Atlantic/Madeira Atlantic/Reykjavik Atlantic/South_Georgia Atlantic/Stanley
 Atlantic/St_Helena Australia/Adelaide Australia/Brisbane Australia/Broken_Hill Australia/Currie
 Australia/Darwin Australia/Eucla Australia/Hobart Australia/Lindeman Australia/Lord_Howe
 Australia/Melbourne Australia/Perth Australia/Sydney Europe/Amsterdam Europe/Andorra
 Europe/Athens Europe/Belgrade Europe/Berlin Europe/Bratislava Europe/Brussels Europe/Bucharest
 Europe/Budapest Europe/Chisinau Europe/Copenhagen Europe/Dublin Europe/Gibraltar
 Europe/Guernsey Europe/Helsinki Europe/Isle_of_Man Europe/Istanbul Europe/Jersey
 Europe/Kaliningrad Europe/Kiev Europe/Lisbon Europe/Ljubljana Europe/London Europe/Luxembourg
 Europe/Madrid Europe/Malta Europe/Mariehamn Europe/Minsk Europe/Monaco Europe/Moscow
 Europe/Oslo Europe/Paris Europe/Podgorica Europe/Prague Europe/Riga Europe/Rome Europe/Samara
 Europe/San_Marino Europe/Sarajevo Europe/Simferopol Europe/Skopje Europe/Sofia
 Europe/Stockholm Europe/Tallinn Europe/Tirane Europe/Uzhgorod Europe/Vaduz Europe/Vatican
 Europe/Vienna Europe/Vilnius Europe/Volgograd Europe/Warsaw Europe/Zagreb Europe/Zaporozhye
 Europe/Zurich Indian/Antananarivo Indian/Chagos Indian/Christmas Indian/Cocos Indian/Comoro
 Indian/Kerguelen Indian/Mahe Indian/Maldives Indian/Mauritius Indian/Mayotte Indian/Reunion
 Pacific/Apia Pacific/Auckland Pacific/Chatham Pacific/Easter Pacific/Efate Pacific/Enderbury
 Pacific/Fakaofu Pacific/Fiji Pacific/Funafuti Pacific/Galapagos Pacific/Gambier Pacific/Guadacanal
 Pacific/Guam Pacific/Honolulu Pacific/Johnston Pacific/Kiritimati Pacific/Kosrae Pacific/Kwajalein
 Pacific/Majuro Pacific/Marquesas Pacific/Midway

Valid Timezones

Pacific/Nauru Pacific/Niue Pacific/Norfolk Pacific/Noumea Pacific/Pago_Pago Pacific/Palau
Pacific/Pitcairn Pacific/Ponape Pacific/Port_Moresby Pacific/Rarotonga Pacific/Saipan Pacific/Tahiti
Pacific/Tarawa Pacific/Tongatapu Pacific/Truk Pacific/Wake Pacific/Wallis